Mail

- Dovecot
  - Anzahl der gleichzeitigen Verbindungen pro IP erhöhen
  - Mails älter als X Tage aus dem Trash löschen
  - Volltextsuche in Mails mit Solr
- Piler
  - Installation von Piler Mailarchive auf Debian Stretch
- Postfix
  - alle ausgehenden Mails an einen festgelegten Empfänger umleiten
  - Disclaimer an ausgehende Mails ranhängen
  - header-Checks
  - Mail aus Mailqueue löschen
  - Mails werden manchmal doppelt zugestellt
  - Mails über ein Relay verschicken, außer bestimmte Empfänger
  - Postfix catch-all Mailaccount
  - Flush mailqueues - Auslieferung erzwingen
- Sendmail
  - Sendmail-Queues
  - Zeitgesteuertes Versenden anhand der Absenderadresse
  - Flush mailqueues - Auslieferung erzwingen
- Cyrus IMAP server
  - CyrusServer DBERROR
  - CyrusServer Mailbox is locked by POP server
- lokales DNS-Black- und Whitelisting mit rbldnsd
- POP3 per Telnet testen
- Procmailrc Beispiele
- Virenscanner auf dem Client verschluckt STARTTLS

Dovecot

Anzahl der gleichzeitigen Verbindungen pro IP erhöhen

Im „protocol imap“-Teil der Config muss die Zeile mail_max_userip_connections ergänzt werden (Dovecot Version 1.2)

/etc/dovecot/dovecot.conf

```
## IMAP specific settings
protocol imap {
  mail_executable = /usr/lib/dovecot/rawlog /usr/lib/dovecot/imap
  mail_plugins = quota imap_quota
  mail_max_userip_connections = 50
}
```

Dovecot

Mails älter als X Tage aus dem Trash löschen

Normalerweise werden Mails, die in den Papierkorb (bei Dovecot üblicherweise .Trash) verschoben wurden, nicht automatisch gelöscht. Über die Zeit sammelt sich dort deshalb ziemlich viel Müll an.

Mit dem folgenden Job lässt sich dort bequem aufräumen:

```
# entweder für alle:
doveadm expunge -A mailbox Trash savedbefore 30d

# oder nur für eine einzelne Mailbox:
doveadm expunge -u user@domain.de mailbox Trash savedbefore 30d
```

Wenn man `expunge` durch `search` ersetzt lässt sich vorher testen, ob wirklich nur die Mails gelöscht werden, die gelöscht werden sollen.

Um es für bequem für mehrere User gleichzeitig zu erledigen habe ich dieses kleine Script gebaut:

```
#!/bin/bash

DAYS=30
USERLIST="user1@domain.de user2@domain.de user3@domain.de"

for user in ${USERLIST}; do
  #doveadm search -u ${user} mailbox Trash savedbefore ${DAYS}d
  doveadm expunge -u ${user} mailbox Trash savedbefore ${DAYS}d
done
```

Volltextsuche in Mails mit Solr

> Diese Anleitung wurde für Debian 8 (Jessie) erstellt.

Versionen:

- Dovecot 2.2.27 (aus den Debian Backports, da die im normalen Debian enthaltene Version ein Problem mit Solr 6.5 hat
- Solr 6.5.1 (Standalone Installation)
- OpenJDK 8 (ebenfalls aus den Backports aufgrund der neueren Version)

Installation/Upgrade Dovecot

Debian Backports aktivieren:

/etc/apt/sources.list.d/backports.list

```
deb http://ftp.de.debian.org/debian jessie-backports main contrib non-free
```

```
aptitude -t jessie-backports install dovecot-core dovecot-solr (+ weitere Pakete, wenn nötig (z.
```

Installation OpenJDK 8

```
aptitude -t jessie-backports install openjdk-8-jdk-headless openjdk-8-jre-headless
```

Installation Solr 6.5.1

Das aktuelle Solr .tgz von apache.org herunterladen und entpacken. Mit dem Installerscript läßt sich der Solr sehr einfach einrichten:

```
cd /root
wget http://mirror.synyx.de/apache/lucene/solr/6.5.1/solr-6.5.1.tgz
tar xvzf solr-6.5.1.tgz
bin/install_solr_service.sh /root/solr-6.5.1.tgz
```

Der Solr-Admin sollte nun über den Browser erreichbar sein: http://localhost:8983

Auf dem Server nun die Datenverzeichnisse anlegen und die Config von Dovecot rüberkopieren:

```
sudo su - solr -c "/opt/solr/bin/solr create -c dovecot -n dovecot"
```

Das Datenverzeichnis liegt in /var/solr/data/dovecot. Bei Solr 6.X kann das Schema über die WebGUI konfiguriert werden. Dovecot kommt aber mit einem eigenen Schema, daher wird beim Deploy dieser Konfiguration diese Möglichkeit deaktiviert.

Nun noch schema.xml und solrconfig.xml nach `/var/solr/data/dovecot/conf` kopieren und die Datei `managed-schema` löschen. Aufgrund der Übersichtlichkeit habe ich diese Dateien im Anhang hinterlegt.

```
cp schema.xml solrconfig.xml /var/solr/data/dovecot/conf
rm /var/solr/data/dovecot/conf/managed-schema
```

Nach einem Neustart des Solr-Services kann Dovecot konfiguriert werden:

```
systemctl restart solr.service
```

Konfiguration von Dovecot

Ich verwende auf dem Dovecot-Server ISPConfig. ISPConfig verwendet nicht das conf.d-Modell mit einzelnen Konfigurationsdateien, sondern packt alles direkt in die `/etc/dovecot/dovecot.conf`. Bitte ändere deine Dateien dort wo notwendig.

/etc/dovecot/dovecot.conf

```
[...]
mail_plugins = quota fts fts_solr
[...]
plugin {
  [...]
  fts = solr
  fts_solr = break-imap-search url=http://localhost:8983/solr/dovecot/
  fts_autoindex = yes
  [...]
}
```

Selbstverständlich können Solr und Dovecot auch auf verschiedenen Servern gehostet werden. Dafür muss nur die IP-Adresse entsprechend angepasst werden. Der Solr-Port (8983) sollte nach außen selbstverständlich mit einer Firewall gesichert werden oder Solr auf eine interne IP gebunden werden. In meinem Setup liegt Solr auf einem internen Server ohne öffentliche IP-Adresse.

Nach einem Neustart per `systemctl restart dovecot.service` kann die Volltextsuche bereits verwendet werden. Dazu muss zuerst der Index erzeugt werden:

```
doveadm index -A -q '*'
```

Da die serverseitige Volltextsuche eine Erweiterung der Suche im IMAP-Protokoll ist, muss ein Client verwendet werden, der dies unterstützt. Mir sind aktuell bekannt: Claws Mail / Sylpheed, Roundcube, Thunderbird.

Piler

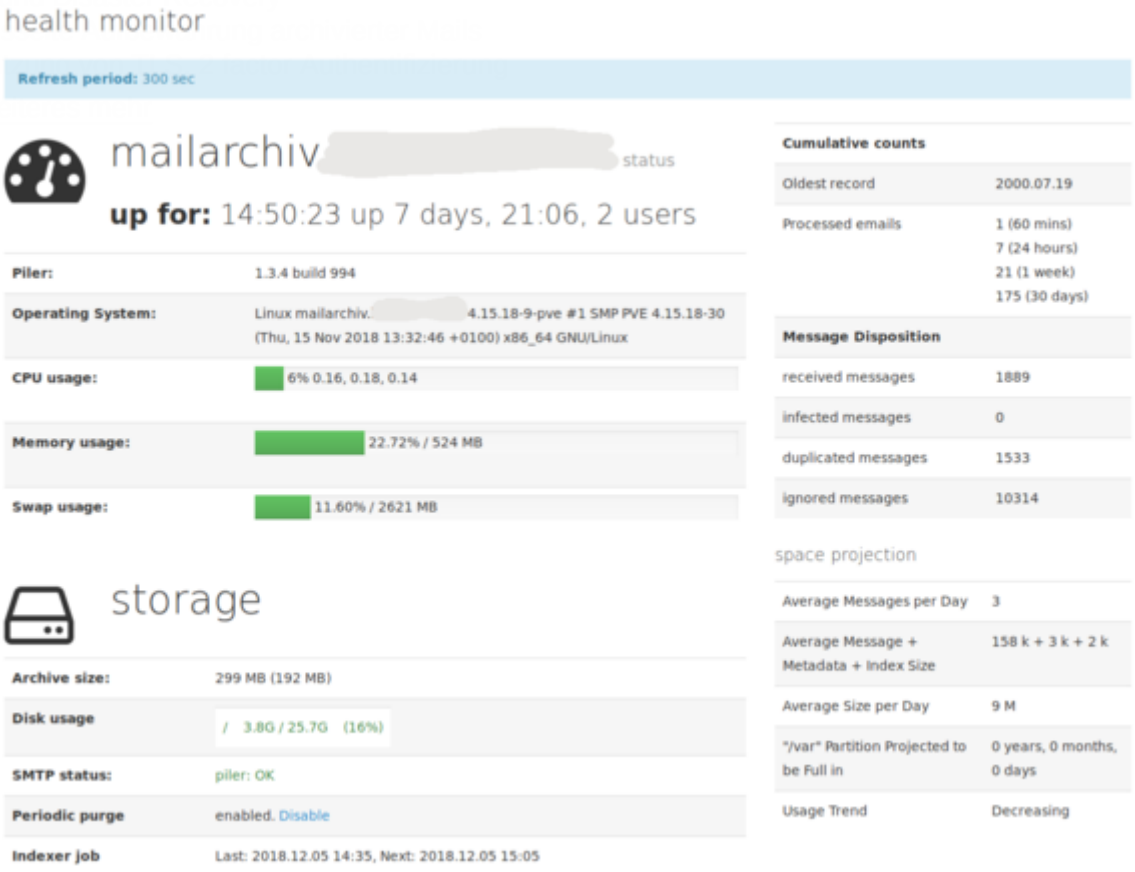
Installation von Piler Mailarchive auf Debian Stretch

Jeder Gewerbetreibende muss Geschäftskorrespondenz für mind. 6 bzw. bis zu 7 Jahre aufheben (Quelle 1, Quelle 2). Wer jetzt nicht all seine Emails ausdrucken und abheften möchte benötigt ein Mailarchiv. Dazu werden einfach alle ein- und ausgehenden Emails zusätzliche zum jeweiligen Empfänger auch an das Archiv geschickt. Ich nutze dafür die Software `piler`, die auf einer virtuellen Maschine läuft. Nach der Installation lauscht piler auf Port 25, nimmt für die konfigurierten Domains Emails an und archiviert diese fälschungssicher.

Piler ist Open Source, bietet eine PHP basierte GUI und unterstützt:

- verschiedene Archivierungs- und Aufbewahrungsregeln
- Deduplikation
- digitaler Fingerprint und Verifizierung
- Volltextsuche in archivierten Mails
- Trennung von Administratoren- und Auditoren- Accounts
- Unterstützung von Google Apps und Office 365
- (Erst-)Import von Mails via IMAP
- Backup und Disaster Recovery
- verschl
- Unterst
- vieles w

Screenshot:



Voraussetzungen

- Ausreichend Diskspace für das Mailarchiv
- Frisches Debian Stretch System, 64-bit
- MariaDB 10.1+
- Sphinx Search 2.2.x
- PHP 7.x
- nginx (geht auch mit Apache oder anderen Webservern)
- ZIP
- mpstat
- python mit mysql

Als Hardware habe ich folgendes gewählt, kommt bei euch natürlich auch etwas auf die Anzahl der Mails an, die verarbeitet werden sollen.

- 2 vCPUs
- 4 GB RAM
- 80 GB Disk

Vor der Installation

Zuerst sollte ein DNS-Eintrag für Piler angelegt werden. Dieser wird benötigt um Mails an Piler weiterleiten zu können und für die GUI.

Installation

Debian Backports aktivieren:

```
deb http://ftp.debian.org/debian stretch-backports main
```

`apt update && apt upgrade`

Postfix muss entfernt werden, da Piler selbst auf Port 25 lauschen mag: `apt purge postfix`

Jetzt müssen noch die notwendigen Pakete installiert werden:

```
apt install nginx openssl libssl-dev mariadb-server default-libmysqlclient-dev sphinxsearch memc
 build-essential python-mysqldb php7.0-fpm php7.0-curl php7.0-gd php7.0-mysql php7.0-cli php7.0-
 php7.0-ldap php7.0-mbstring php-memcached libtre-dev sysstat gcc libwrap0 libwrap0-dev latex2rt
 catdoc poppler-utils unrtf tnef unixodbc libpq5 libzip-dev libzip4 zipcmp zipmerge ziptool
```

Der automatische Start von Sphinx muss ausgeschaltet bleiben, bitte prüfe ob in `/etc/default/sphinxsearch` der Eintrag `„START=no“` hinterlegt ist.

Gruppe und Benutzer anlegen:

```
groupadd -r piler
useradd -r -g piler -m -s /bin/sh -d /var/piler piler
usermod -L piler
chmod 0755 /var/piler
```

Piler herunterladen und kompilieren. Den aktuellen Tarball gibts immer hier. Als root:

```
wget https://bitbucket.org/jsuto/piler/downloads/piler-1.3.4.tar.gz
tar xvzf piler-1.3.4.tar.gz
cd piler-1.3.4/
./configure \
  --localstatedir=/var \
  --with-database=mysql \
  --enable-tcpwrappers \
  --enable-memcached
make
make install
ldconfig
```

Konfiguration

Damit der Postinstall problemlos durchläuft sollte die root-Shell noch von dash auf bash gesetzt werden: `dpkg-reconfigure dash` –> NO auswählen (also bash verwenden). Danach einmal aus- und wieder einloggen.

Der Postinstall kommt leider noch nicht mit dem MySQL auth-socket ab Debian Stretch klar, daher habe ich hier eine gepatchte Version zur Verfügung gestellt. Der Postinstall kümmert sich um die Einrichtung der MySQL-Datenbank, Sphinx, ggf. einem Smarthost/Relayhost und die WebGUI.

```
make postinstall


This is the postinstall utility for piler
It should be run only at the first install. DO NOT run on an existing piler installation!


Continue? [Y/N] [N] y


Please enter the webserver groupname [www-data]

Please enter mysql hostname [localhost]

Please enter mysql socket path [/var/run/mysqld/mysqld.sock]

Please enter mysql database [piler]

Please enter mysql user name [piler]

Please enter mysql password for piler [] <geheimespasswort>
mysql connection successful


Please enter the path of sphinx.conf [/usr/local/etc/piler/sphinx.conf]

Please enter smtp relay []

Please enter smtp relay port [25]
no crontab for piler



INSTALLATION SUMMARY:

piler user: piler
keyfile: /usr/local/etc/piler/piler.key

mysql host: localhost
mysql socket: /var/run/mysqld/mysqld.sock
mysql database: piler
mysql username: piler
mysql password: *******

sphinx indexer: /usr/bin/indexer
sphinx config file: /usr/local/etc/piler/sphinx.conf

vhost docroot: /var/www/piler
www group: www-data

smtp relay host:
```

```
smtp relay port: 25

piler crontab:
### PILERSTART
5,35 * * * * /usr/local/libexec/piler/indexer.delta.sh
30   2 * * * /usr/local/libexec/piler/indexer.main.sh
15,45 * * * * /usr/local/libexec/piler/indexer.attachment.sh
*/15 * * * * /usr/bin/indexer --quiet tag1 --rotate --config /usr/local/etc/piler/sphinx.conf
*/15 * * * * /usr/bin/indexer --quiet note1 --rotate --config /usr/local/etc/piler/sphinx.conf
30   6 * * * /usr/bin/php /usr/local/libexec/piler/generate_stats.php --webui /var/www/piler >/d
*/5 * * * * /usr/bin/find /var/www/piler/tmp -type f -name i.\* -exec rm -f {} \;
### PILEREND



Correct? [Y/N] [N] y

Continue and modify system? [Y/N] [N] y

Creating mysql database... Done.
Writing sphinx configuration... Done.
Initializing sphinx indices... Sphinx 2.2.11-id64-release (95ae9a6)
Copyright (c) 2001-2016, Andrew Aksyonoff
Copyright (c) 2008-2016, Sphinx Technologies Inc (http://sphinxsearch.com)

using config file '/usr/local/etc/piler/sphinx.conf'...
indexing index 'main1'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.002 sec, 0 bytes/sec, 0.00 docs/sec
indexing index 'main2'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.000 sec, 0 bytes/sec, 0.00 docs/sec
indexing index 'main3'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.000 sec, 0 bytes/sec, 0.00 docs/sec
indexing index 'main4'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.000 sec, 0 bytes/sec, 0.00 docs/sec
indexing index 'dailydelta1'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.000 sec, 0 bytes/sec, 0.00 docs/sec
indexing index 'delta1'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.002 sec, 0 bytes/sec, 0.00 docs/sec
indexing index 'tag1'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.000 sec, 0 bytes/sec, 0.00 docs/sec
indexing index 'note1'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.000 sec, 0 bytes/sec, 0.00 docs/sec
indexing index 'att1'...
collected 0 docs, 0.0 MB
total 0 docs, 0 bytes
total 0.001 sec, 0 bytes/sec, 0.00 docs/sec
total 9 reads, 0.000 sec, 0.0 kb/call avg, 0.0 msec/call avg
total 63 writes, 0.000 sec, 0.0 kb/call avg, 0.0 msec/call avg
Done.
installing cron entries for piler... Done.
installing keyfile (piler.key) to /usr/local/etc/piler/piler.key... Done.
Making an ssl certificate ... Generating a RSA private key
.....................................................................................
.....................................................................................
writing new private key to '/usr/local/etc/piler/piler.pem'
-----
Copying www files to /var/www/piler... Done.

Done post installation tasks.
```

In der Konfigurationsdatei `/usr/local/etc/piler/piler.conf` muss noch die passende hostid hinterlegt werden. Dazu wird die Datei im Texteditor geöffnet und etwa in Zeile 14 die hostid auf den Hostnamen deines Pilers gesetzt (z.B. piler.mydomain.de). Außerdem legen wir hier gleich den Zeitraum fest für den Mails aufgehoben werden sollen: `default_retention_days=2557`.

Außerdem scheint beim postinstall-Script eine Variablenersetzung nicht zu klappen, daher muss noch die Konfiguration der WebUI angepasst werden. In `/var/www/piler/config.php` etwa in Zeile 321 steht `${prefix}` das durch den vollständigen Pfad zur config-site.php ersetzt werden muss, z.B:

```
-require_once '${prefix}/etc/piler/config-site.php';
+require_once '/var/www/piler/config-site.php';
```

Der nginx-Vhost schaut bei mir so aus:

```
server {
  server_name piler.mydomain.de;

  root /var/www/piler;

  access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;

  gzip on;
  gzip_types text/plain application/xml text/css;
  gzip_vary on;

  location / {
    index  index.php index.html;
    try_files $uri $uri/ /index.php;
  }

  error_page   500 502 503 504  /50x.html;
  location = /50x.html {
    root   html;
  }

  location ~ [^/]\.php(/|$) {
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;

    fastcgi_split_path_info ^(.+?\.php)(/.*)$;
    if (!-f $document_root$fastcgi_script_name) {
      return 404;
    }

    fastcgi_pass unix:/var/run/php/php7.0-fpm.sock;
    fastcgi_index index.php;
    include fastcgi_params;
  }

  location ~* \.(ico|css|js|gif|jpe?g|png)$ {
    expires 2w;
  }

  rewrite /search.php /index.php?route=search/search&type=simple;
  rewrite /advanced.php /index.php?route=search/search&type=advanced;
  rewrite /expert.php /index.php?route=search/search&type=expert;
  rewrite /search-helper.php /index.php?route=search/helper;
  rewrite /audit-helper.php /index.php?route=audit/helper;
  rewrite /message.php /index.php?route=message/view;
  rewrite /bulkrestore.php /index.php?route=message/bulkrestore;
  rewrite /bulkremove.php /index.php?route=message/bulkremove;
  rewrite /bulkpdf.php /index.php?route=message/bulkpdf;
  rewrite /folders.php /index.php?route=folder/list&;
  rewrite /settings.php /index.php?route=user/settings;
  rewrite /login.php /index.php?route=login/login;
  rewrite /logout.php /index.php?route=login/logout;
  rewrite /google.php /index.php?route=login/google;
  rewrite /domain.php /index.php?route=domain/domain;
  rewrite /ldap.php /index.php?route=ldap/list;
  rewrite /customer.php /index.php?route=customer/list;
  rewrite /retention.php /index.php?route=policy/retention;
  rewrite /archiving.php /index.php?route=policy/archiving;
```

```
  rewrite /legalhold.php /index.php?route=policy/legalhold;
  rewrite /view/javascript/piler.js /js.php;
}
```

Jetzt nicht vergessen den Vhost zu aktivieren und nginx zu reloaden:

```
ln -s /etc/nginx/sites-available/test-piler1.wavecloud.de /etc/nginx/sites-enabled/
nginx -t
nginx -s reload
```

Init-Scripte (Systemd-Unit files werden keine mitgeliefert) kopieren und aktiveren:

```
cp init.d/rc.piler /etc/init.d/
cp init.d/rc.searchd /etc/init.d
systemctl daemon-reload
systemctl enable rc.piler.service
systemctl enable rc.searchd.service
systemctl start rc.piler.service
systemctl start rc.searchd.service
```

Die GUI sollte nun über den Browser erreichbar sein: `http://piler.mydomain.de/`. Es empfiehlt sich der Seite noch eine passende SSL/TLS-Konfiguration zu spendieren.

Die Standardbenutzername lautet **admin@local** / **pilerrocks** und sollte gleich geändert werden. Es sollte gleich auch ein Kennwort für den Standardauditor gesetzt werden. Die Rolle „Master admin“ darf verwalten und administrieren. Die Rolle „Auditor“ wird verwendet um auf Mails im Archiv zuzugreifen. Beide haben unterschiedliche Oberflächen.

Ich habe noch folgende Einstellungen in der GUI vorgenommen:

- administration ? domain: Hinzugefügt `ovtec.it` / mapped domain: `ovtec.it`
- administration ? archiving rules: Hier werden Regeln eingetragen, deren Ziele NICHT archiviert werden (z.B. CRON-Mails usw.)
- administration ? retention rules: Ist hier nicht eingetragen gilt der Standardwert aus der piler.conf (2557 Tage)

Der Host sollte nun noch einmal abschließend rebootet werden, danach prüfen ob alle Dienste laufen:

```
# ps ax | grep -E "piler|searchd|mysql|nginx"
  445 ?        Ssl    0:00 /usr/sbin/mysqld
  448 ?        S      0:00 searchd --config /usr/local/etc/piler/sphinx.conf
  449 ?        Sl     0:00 searchd --config /usr/local/etc/piler/sphinx.conf
  453 ?        Ss     0:00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on
  454 ?        S      0:00 nginx: worker process
  455 ?        S      0:00 nginx: worker process
  505 ?        Ss     0:00 /usr/local/sbin/piler-smtp -d
  508 ?        Ss     0:00 /usr/local/sbin/piler -d
  509 ?        S      0:00 /usr/local/sbin/piler -d
  510 ?        S      0:00 /usr/local/sbin/piler -d
```

Alle Mails, die nun an bspw. archive@piler.mydomain.de geschickt werden und mit einer der in `Domains` konfigurierten Domains übereinstimmen werden entsprechend den eingestellten Regeln archiviert. Es gibt verschiedene Wege, wie Mails weitergeleitet werden können. Die Piler-Dokumentation führt dazu einige auf.

Dokumentation

Hier noch ein paar Links zur Piler Dokumentation:

- Installation
- FAQ
- Übersicht

Postfix

Postfix

alle ausgehenden Mails an einen festgelegten Empfänger umleiten

Vor allem auf Entwicklungsservern macht es oft Sinn, dass alle Mails, die diese Server verschicken sollen, nur an einen vorher festgelegten Empfänger gehen, um z.B. echte Kunden nicht zu belästigen oder ungewollte Bestellungen aufzugeben.

Alle Mail soll an entwicklung@meinedomain.de gehen.

Folgende Files müssen angepasst oder erstellt werden:

```
always_bcc=entwicklung@meinedomain.de
transport_maps = hash:/etc/postfix/transport
```

Dies bewirkt, dass alle Mails per BCC an entwicklung@meinedomain.de geschickt werden. Jetzt muss nur noch verhindert werden, dass die echten Mails verschickt werden. Dazu folgendes Transport-File erstellen /etc/postfix/transport

```
entwicklung@meinedomain.de : * discard:silently
```

Die erste Zeile sorgt dafür, dass Mails an entwicklung@meinedomain.de auf normalem Weg zugestellt werden. Zeile 2 wirft alle anderen Mails weg.

Das transport-File muss jetzt nur noch gehasht (postmap /etc/postfix/transport) und der Postfix reloaded werden (/etc/init.d/postfix reload).

Die korrekte Funktionalität kann man natürlich in /var/log/mail.log überwachen.

Disclaimer an ausgehende Mails ranhängen

Postfix selbst läßt keine Änderung des Bodies durchlaufender Mails zu. Um einen Disclaimer oder sonstigen Text ans Ende jeder Mail zu hängen bedienen wir uns des Tools „altermime“ und konfigurieren im Postfix einen zusätzlichen Content-Filter.

Postfix master.cf, ändern der Zeile smtp (-o content_filter hinzufügen):

```
smtp      inet  n       -       n       -       -       smtpd
  -o content_filter=dfilt:
```

Am Ende der Datei folgenden Eintrag hinzufügen:

```
dfilt     unix    -       n       n       -       -       pipe
    flags=Rq user=filter argv=/etc/postfix/disclaimer -f ${sender} -- ${recipient}
```

Erstellen des disclaimer-Scripts /etc/postfix/disclaimer mit folgendem Inhalt:

```
#!/bin/sh
# Localize these.
INSPECT_DIR=/var/spool/filter
SENDMAIL="/usr/sbin/sendmail -G -i"

# don't alter mails from the addresses in this file
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses

# Exit codes from <sysexits.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15

# Start processing.
cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; exit
$EX_TEMPFAIL; }

cat >in.$$ || { echo Cannot save mail to file; exit $EX_TEMPFAIL; }

# obtain From address
from_address=`grep -m 1 "^From:" in.$$ | cut -d "<" -f 2 | cut -d ">" -f 1  | sed 's/^From: //g'

if [ ! `grep -wi ^${from_address}$ ${DISCLAIMER_ADDRESSES}` ]; then
  /usr/bin/altermime --input=in.$$ \
                     --disclaimer=/etc/postfix/disclaimer.txt \
                     --disclaimer-html=/etc/postfix/disclaimer.txt || \
                     { echo Message content rejected; exit $EX_UNAVAILABLE; }
fi

$SENDMAIL "$@" <in.$$

exit $?
```

Das Script jetzt nocht ausführbar machen („chmod og+x /etc/postfix/disclaimer; chgrp filter /etc/postfix/disclaimer“).

Anlegen einer Datei mit dem Disclaimertext /etc/postfix/disclaimer.txt:

```
Testfirma
Blastraße 1
12345 Blastadt

Alle Rechte vorbehalten!
```

Anlegen einer Datei /etc/postfix/disclaimer_addresses mit Mailadressen, die NICHT mit einem Disclaimer versehen werden sollen:

```
noreply@testfirma.de
```

Jetzt noch den Postfix reloaden (service postfix reload). Nun werden alle Mails, deren Absender nicht mit einer Adresse aus disclaimer_addresses übereinstimmt, mit dem konfigurierten Disclaimer versehen.

Wenn die Funktion von „disclaimer_addresses“ umgedreht werden soll, sprich nur Mails von Absendern, die in der Datei enthalten sind, werden mit einem Disclaimer versehen, dann muss nur das „!“ in Zeile 34 entfernt werden.

> Da altermime den Body der Mail verändert könnnen PGP-verschlüsselte Mails hinterher nicht mehr entschlüsselt werden!

header-Checks

Ein Beispiel für die Datei /etc/postfix/header_checks

```
IF /^Subject:/

/^Subject: Belebt Geist und Korper/                          REJECT  Message content rejected;
/^Subject: Bitte tiefer eindringen und abladen/              REJECT  Message content rejected;
/^Subject: Nie mehr zu fruh kommen/                          REJECT  Message content rejected;
/^Subject: Privatkredite/                                    REJECT  Message content rejected;
/^Subject: schoolgirls/                                      REJECT  Message content rejected;
/^Subject: Russian/                                          REJECT  Message content rejected;
/^Subject: Potenzprobleme/                                   REJECT  Message content rejected;
/^Subject: Probieren Sie es/                                 REJECT  Message content rejected;
/^Subject: Teenage/                                          REJECT  Message content rejected;
/^Subject: Spitzenduell/                                     REJECT  Message content rejected;
/^Subject: Energy/                                           REJECT  Message content rejected;
/^Subject: sparen/                                           REJECT  Message content rejected;
/^Subject: Banish/                                           REJECT  Message content rejected;
/^Subject: rufen/                                            REJECT  Message content rejected;
/^Subject: Rabatte/                                          REJECT  Message content rejected;
/^Subject: safe/                                             REJECT  Message content rejected;
/^Subject: Ficken/                                           REJECT  Message content rejected;
/^Subject: Financial/                                        REJECT  Message content rejected;
/^Subject: girl/                                             REJECT  Message content rejected;
/^Subject: Happy/                                            REJECT  Message content rejected;
/^Subject: Newsletter/                                       REJECT  Message content rejected;
/^Subject: lebt/                                             REJECT  Message content rejected;
/^Subject: Man/                                              REJECT  Message content rejected;
/^Subject: PAYMENT/                                          REJECT  Message content rejected;
/^Subject: Pedolover/                                        REJECT  Message content rejected;
/^Subject: Pedo/                                             REJECT  Message content rejected;
/^Subject: Medically/                                        REJECT  Message content rejected;
/^Subject: Pics/                                             REJECT  Message content rejected;
/^Subject: %/                                                REJECT  Message content rejected;
ENDIF
```

Einzelne Regeln lassen sich auch folgendermaßen testen:

```
echo 'Subject: Belebt Geist und Korper' | postmap -fq - pcre:/etc/postfix/header_checks
```

Mail aus Mailqueue löschen

Als Admin kennt man das. Mal ein durchdrehendes Script, mal ein Spamopfer… Gelegentlich ist es nötig Mails schnell aus der Postfix-Queue zu löschen.

Alle Mails aus der Queue löschen

Das könnte wichtig werden, wenn die Queue eigentlich nur mit double-bounces verstopft ist. Achtung, dieses Kommando räumt die Queue richtig auf.

```
postsuper -d ALL
```

Alle Mails mit bestimmten Inhalt löschen

Wenn z.B. ein Kontaktformular eines Forum missbraucht wurde und in allen (ungewünschten) Mails der gleiche Text vorkommt.

```
grep -rl "Ein netter Gruss von" * | cut -d"/" -f2 | postsuper -d -
```

Mail mit bestimmten Sender oder Empfänger löschen

Dies löscht Mails mit einem bestimmten Sender oder Empfänger:

```
postqueue -p | tail -n +2 | awk 'BEGIN { RS = "" } /@yahoo\.it$/ { print $1 }' | tr -d '*!' | postsuper -d -
```

Mail an bestimmten Empfänger löschen

Als Einzeiler:

```
postqueue -p | grep -v '^ *(' | awk 'BEGIN { RS = "" } { if ($8 == "benutzer@deinserver.de")print $1 }' | tr -d '*!'
| postsuper -d -
```

Oder über ein Perl-Script mit einem regulären Ausdruck:

```
#!/usr/bin/perl

$REGEXP = shift || die "no email-adress given (regexp-style, e.g. bl.*\@yahoo.com)!";

@data = qx</usr/sbin/postqueue -p>;
for (@data) {
  if (/^(\w+)(\*|\!)?\s/) {
     $queue_id = $1;
  }
  if($queue_id) {
    if (/$REGEXP/i) {
      $Q{$queue_id} = 1;
```

```
      $queue_id = "";
    }
  }
}

#open(POSTSUPER,"|cat") || die "couldn't open postsuper" ;
open(POSTSUPER,"|postsuper -d -") || die "couldn't open postsuper" ;

foreach (keys %Q) {
  print POSTSUPER "$_\n";
};
close(POSTSUPER);
```

Postfix

Mails werden manchmal doppelt zugestellt

Manchmal werden Mails doppelt zugestellt, dies wird durch die doppelte Auswertung der virtual_alias_maps in Postfix, einmal vor dem content_filter, und dann nach dem content_filter, wenn Amavisd-new die Mail wieder an Postfix zurückgibt, hervorgerufen.

Um dies abzustellen muss in der /etc/postfix/master.cf folgendes konfiguriert werden:

```
[...]
127.0.0.1:10025 inet n  -       n     -       -  smtpd
     -o content_filter=
     -o local_recipient_maps=
     -o relay_recipient_maps=
     -o smtpd_restriction_classes=
     -o smtpd_delay_reject=no
     -o smtpd_client_restrictions=permit_mynetworks,reject
     -o smtpd_helo_restrictions=
     -o smtpd_sender_restrictions=
     -o smtpd_recipient_restrictions=permit_mynetworks,reject
     -o smtpd_data_restrictions=reject_unauth_pipelining
     -o smtpd_end_of_data_restrictions=
     -o mynetworks=127.0.0.0/8
     -o smtpd_error_sleep_time=0
     -o smtpd_soft_error_limit=1001
     -o smtpd_hard_error_limit=1000
     -o smtpd_client_connection_count_limit=0
     -o smtpd_client_connection_rate_limit=0

Hinzufügen:
     -o receive_override_options=no_address_mappings
```

falls es die Zeile „-o receive_override_options=“ bereits gibt, muss „no_address_mappings“ einfach durch Komma getrennt hinten angehängt werden.

Mails über ein Relay verschicken, außer bestimmte Empfänger

Alle ausgehenden Mails sollten über ein Relay verschickt werden. Nur Mails an bestimmte Empfänger sollen direkt zugestellt werden.

In der Postfix-Standardkonfiguration werden noch folgende Anpassungen gemacht:

an /etc/postfix/main.cf wird folgende Zeile angehängt. Die Variable relay_host wird nicht konfiguriert

```
transport_maps = hash:/etc/postfix/transport
```

Empfänger, an die direkt zugestellt werden soll, werden in der Datei /etc/postfix/transport eingetragen. Das Standard-Relay wird die letzte Zeile in der Datei

```
testuser@domain1.de :
direkt@domain2.de :
* smtp:mein.relay.de
```

Nun muss noch das File-Hash erzeugt werden:

```
postmap /etc/postfix/transport
```

und die Postfix Konfiguration neu geladen werden:

```
/etc/init.d/postfix reload
```

jetzt einige Testmails verschicken und den Weg in /var/log/mail.log überprüfen:

```
direkt:
echo "Testmail direkt" | mail -s Test1 direkt@domain2.de

über das Relay:
echo "Testmail relay" | mail -s Test2 nichtdirekt@domain2.de
```

Postfix

Postfix catch-all Mailaccount

Dies beschreibt die Einrichtung eines catch-all Mailaccounts im Postfix-MTA

- Als root die Datei /etc/postfix/main.cf bearbeiten und folgenden Eintrag vornehmen/aktivieren:

```
virtual_alias_maps = hash:/etc/postfix/virtual
```

- in der Datei /etc/postfix/virtual werden nun die die virtuellen Accounts definiert:

```
# lokale user
heinz@server.de     heinz
bert@server.de      bert
schwuffi@server.de  schwuffi

# catch-all
@server.de          mailsammler
```

- um daraus das DB-File für Postfix zu erzeugen:

```
postmap /etc/postfix/virtual
```

- jetzt noch den Postfix reloaden mit:

```
postfix reload
```

Postfix

Flush mailqueues - Auslieferung erzwingen

ganz einfach über folgenden Befehl:

```
postqueue -f
```

Um die Queue betrachten und z.B. nur einzelne Mails zu flushen oder auf HOLD zu setzen, bietet sich das Tool „pfqueue“ an, dass bei allen gängigen Distris in den Repos enthalten sein sollte.

Sendmail

Sendmail-Queues

Das Aufteilen eingehender bzw. zu versendender Mails ist für hochfrequentierte Mailserver nützlich. Sendmail verschickt Mails anhand ihrer Priorität, die aus folgenden Faktoren berechnet wird:

- Größe der Email
- Priorität (kann im Mailer eingestellt werden)
- Anzahl der Empfänger
- Wie lange ist die Mail schon in der Queue? Jeder Zustellungsversuch verringert die Priorität

Je höher dieser Prioritätswert ist, desto niedriger ist die Priorität mit der sendmail diese Mail behandelt.

Hat man nun ein hochfrequentiertes System und eine Mail konnte mehrmals nicht zugestellt werden, kann es durchaus sein, dass diese Mail lange Zeit in der Queue festhängt.

Abhilfe schafft hier die Konfiguration weiterer Mailqueues, die mit unterschiedlichen Wiederholungszeiten abgearbeitet werden. Hierzu wird in der sendmail.mc folgender Eintrag vorgenommen:

```
FEATURE(`queuegroup')
QUEUE_GROUP(`mqueue', `P=/var/spool/mqueue/mqueue, R=5, r=15, F=f, Interval=1h')
QUEUE_GROUP(`fast', `P=/var/spool/mqueue/fast, R=5, r=15, F=f, Interval=5m')
QUEUE_GROUP(`cno', `P=/var/spool/mqueue/cno, R=5, r=15, F=f, Interval=15m')
```

in access:

```
QGRP:default                    mqueue
QGRP:de                         fast
QGRP:wichtig.com                fast
QGRP:auchwichtig.org            fast
QGRP:com                        cno
QGRP:net                        cno
QGRP:org                        cno
```

danach mit „make“ (das sendmail-cf paket muss installiert sein) die Konfiguration neu bauen.

Die Standardgruppe ist mqueue, diese wird stündlich abgearbeitet. Hier wandern alle Mails rein, die auf keine der anderen Queues zutreffen. Alle Mails an .de-Adressen / wichtig.com und auchwichtig.org werden in die fast-Queue einsortiert und alle 5 Minuten abgearbeitet. Mails an .com/.net/.org-Adressen wandern in die cno-Queue und werden alle 15 Minuten abgearbeitet.

Zeitgesteuertes Versenden anhand der Absenderadresse

Diese Anleitung wurde für CentOS 5.5 geschrieben, unter anderen Distribution sollte das mit etwas Mitdenken genauso möglich sein.

Dieses Szenario beschreibt ein Mailrelay, welches eingehende Mails erstmal in eine Queue schiebt, die dann später zeitgesteuert z.B. per Cron abgearbeitet wird.

http://www.murty.net/qgrpx/

Es sind mehrere Queues mit verschiedenen Zeiten möglich. Das Einsortieren in die Queues kann anhand folgender Kriterien konfiguriert werden (das Standard-CF queuegroup kann nur mit Zieldomains umgehen, für die Sortierung anhand Absenderadresse muss die Erweiterung queuegroupx installiert werden):

```
QFTO:sender@senderdomain.com<@>recipient@recipientdomain.com  qg1
QFTO:<><@>recipient1@recipientdomain1.com                     qg2
QFRM:sender1@senderdomain1.com                                qg3
QFRM:senderdomain2.com                                        qg4
QFRM:<>                                                       qg5
QGRP:recipient2@recipientdomain2.com                          qg6
QGRP:recipientdomain3.com                                     qg
```

Installation und Konfiguration

Das bei sendmail mitgelieferte CF-Script queuegroup kann die Sortierung nur anhand der Zieldomain erledigen (QGRP:recipientdomain3.com qg). Werden die anderen Kriterien benötigt muss die Erweiterung queuegroupx von http://www.murty.net/qgrpx/ installiert werden. Dort steht auch, wie die Erweiterung installiert werden muss. Für CentOS reichts aus, die m4-Datei nach /usr/share/sendmail-cf/feature/queuegroupx.m4 zu legen.

Zuerst müssen die Verzeichnisse für die neuen Queues angelegt und berechtigt werden. Die Default-Queue wandert von /var/spool/mqueue/ nach /var/spool/mqueue/default. Die weiteren Verzeichnisse sind für unserer Queues:

```
cd /var/spool/mqueue
mkdir default
mkdir adminmails
mkdir apache
chown root.mail *
chmod go-rwx *
```

In die Datei /etc/mail/sendmail.mc werden folgende Zeilen (ca. ab Zeile 101, unter FEATURE access_db) eingefügt. Achtung, hier wird beim FEATURE zwischen queuegroup und queuegroupx unterschieden!

```
dnl #
dnl # just queue incoming mails, they are send via cron
define(`confDELIVERY_MODE', `q')dnl
dnl #
dnl # queuegroups for the different senders
FEATURE(queuegroupx)dnl
QUEUE_GROUP(`mqueue', `P=/var/spool/mqueue/default, R=5, r=15, F=f, Interval=1h')dnl
QUEUE_GROUP(`adminmails', `P=/var/spool/mqueue/adminmails, R=5, r=15, F=f, Interval=1h')dnl
```

```
QUEUE_GROUP(`apache', `P=/var/spool/mqueue/apache, R=5, r=15, F=f, Interval=1h')dnl
dnl #
```

der DeliveryMode wird auf q gesetzt, d.h. alle eingehenden Mails werden nur in eine Queue gesteckt und nicht weiter bearbeitet. Danach werden die verschiedenen Queues konfiguriert.

In der Datei /etc/mail/access müssen jetzt noch die Kriterien für die Sortierung konfiguriert werden (ich verwende hier queuegroupx für die Sortierung anhand des Absenders):

```
QFRM:root@localhost       adminmails
QFRM:apache@localhost     apache
```

Alle Mails, die keine Treffer bei den obigen Regeln haben, werden in die Standardqueue mqueue einsortiert.

Damit der Server auch als Relay verwendet werden kann, müssen noch die erlaubten Netze konfiguriert werden, aus denen Mails eingeliefert werden dürfen (oder ihr konfiguriert SMTP-Auth):

In /etc/mail/access z.B. folgendes eintragen, um den Servern in den Netzen 192.168.60.0/24 und 10.11.12.0/24 das relayen von Mail über diesen Server zu erlauben:

```
Connect:192.168.60   RELAY
Connect:10.11.12   RELAY
```

Außerdem muss sendmail noch so konfiguriert werden, dass es auch auf den externen IP-Adressen lauscht. Dazu in /etc/mail/sendmail.mc die folgende Datei auskommentieren.

```
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
```

jetzt muss nur noch ein Cronjob konfiguriert werden, der den Queuerun startet, damit die Mails auch verschickt werden:

```
*/30 * * * * sendmail -vqR -qGmqueue
0 0 * * * sendmail -vqR -qGadminmails
0 0 * * * sendmail -vqR -qGapache
```

Sendmail

Flush mailqueues - Auslieferung erzwingen

Bei sendmail geht das Leeren der Queue über folgenden Befehl:

```
sendmail -vqR
```

einzelne Mails zu flushen geht AFAIK nicht, aber für eine bestimmte Domain ist es kein Problem:

```
sendmail -vqRmagenbrot.net
```

Cyrus IMAP server

CyrusServer DBERROR

Cyrus bringt folgende Fehlermeldungen im maillog:

```
Jan  7 04:04:13 server master[29039]: about to exec /usr/lib/cyrus-imapd/lmtpd
Jan  7 04:04:13 server lmtp[29039]: executed
Jan  7 04:04:13 server lmtp[29039]: DBERROR 0?      : db4
Jan  7 04:04:13 server lmtp[29039]: DBERROR: opening /var/lib/imap/deliver.db: Cannot allocate m
Jan  7 04:04:13 server lmtp[29039]: DBERROR: opening /var/lib/imap/deliver.db: cyrusdb error
Jan  7 04:04:13 server lmtp[29039]: FATAL: lmtpd: unable to init duplicate delivery database
Jan  7 04:04:13 server master[3516]: process 29039 exited, status 75
Jan  7 04:04:13 server master[3516]: service lmtp pid 29039 in READY state: terminated abnormall
```

Ursache kann wohl niemand so richtig festlegen, aber ein einfacher Neustart des Cyrus-Daemons bringt Abhilfe.

CyrusServer Mailbox is locked by POP server

Problem: User kann seine Mails via POP3 nicht mehr vom Server holen

Fehlermeldung im Client: „Mailbox is locked by POP server“

Mögliche Ursache: Client hat unerwarteterweise die Verbindung beendet, POP3-Lock bleibt dennoch bestehen

Lösung: mit folgendem Befehl lassen sich die letzten Logins auf dieses Konto anzeigen (Username ersetzen):

```
egrep '^.*pop3.*login: .*<username>.*$' /var/log/maillog
```

hier stehen die PIDs für den zugehörigen pop3-Prozess in den [] Klammern. Nun einfach die PIDs von unten angefangen killen bis der Zugriff auf die Mailbox wieder möglich ist.

lokales DNS-Black- und Whitelisting mit rbldnsd

Manchmal ist es nötig, bestimmte IP-Netze, die zwar viel Spam verschicken, aber dennoch nirgends gelistet werden, manuell auf eine eigene Blacklist zu setzen. Dann gibts da auch IP-Netze, z.B. von Orange in Frankreich, die den zahlenden Kunden zur Verfügung gestellt werden, über die dann aber auch soviel Müll verschickt wird, dass diese regelmäßig (zurecht) auf irgendwelchen Listen landen.

Hier will ich nun kurz zeigen, wie man sich für diese zwecke einen eigenen DNS-Blacklisting bzw. DNS-Whitelisting Server aufsetzt.

Installation

Ich habs unter Fedora 4 getestet, neuere Versionen weichen möglicherweise ab:

```
yum -y install rbldnsd
```

Konfiguration

Die Konfiguration ist sehr einfach gehalten. Über die Datei /etc/sysconfig/rbldnsdd werden nur einige Parameter gesetzt. Ich habe hier ein Setup mit nur einer Zone für eine DNS-Whitelist, zu Dokumentationszwecken habe ich trotzdem mal die komplette Datei mit Kommentaren eingefügt:

```
# /etc/default/rbldnsd
# This file should set one variable, RBLDNSD, to be a multiline
# list of all instances of rbldnsd to start.  Every line in that
# list consist of a key (basename for a pid file), and rbldnsd
# command line, e.g.:
#
RBLDNSD="dnswl -r /var/lib/rbldnsd/dnswl -q -b 127.0.0.1 dnswl.magenbrot.net:ip4set:dnswl.magenb
#
# or, using multiple lines and line continuations:
#
# RBLDNSD="dsbl -r/var/lib/rbldnsd/dsbl -q -b 127.2 \
#   list.dsbl.org:ip4set:list \
#   multihop.dsbl.org:ip4set:multihop \
#   unconfirmed.dsbl.org:ip4set:unconfirmed \
#
# local -r/var/lib/rbldnsd/local -q -b 127.3 \
#   dialups.bl.example.com:ip4set:dialups \
#   spews.bl.example.com:ip4set:spews \
#   inputs.bl.example.com:ip4set:inputs \
#   bl.example.com:ip4set:dialups \
#   bl.example.com:ip4set:spews \
#   bl.example.com:ip4set:inputs \
#
#  "
#
# This is the recommended way to keep entries readable and
# easily editable.
#
# the first word, key, will be used to form pid file name, like
# /var/run/rbldnsd-dsbl.pid, /var/run/rbldnsd-local.pid etc.
# So, all keys should be unique.  This is done in order to support
# several instances of rbldnsd, if that'll be required.  In a
```

```
# simple case, when only one instance is needed, key may be
# specified as a single dash, -, and in this case pid file
# will be /var/run/rbldnsd.pid :
#
# RBLDNSD="- -r/var/lib/rbldnsd -q -b127.2 \
#   zone list...\
# "
#
# See rbldnsd(8) for descriptions of options.
#
```

wichtig ist hier nur die eine Zeile, deren Format ich hier kurz erkläre:

```
RBLDNSD="dnswl -r /var/lib/rbldnsd/dnswl -q -b 127.0.0.1 dnswl.magenbrot.net:ip4set:dnswl.magenb
         key der zone fuers pidfile      |  |            |
               chroot-verzeichnis        |  |            |
                                         |zuerst in den hintergrund wechseln, dann die zonen lad
                                            |nur auf dieser Adresse lauschen
                                                         |Zonenname:Typ:Filename
```

Zonefile erzeugen

jetzt muss noch das Zonefile erstellt werden. Für das obige Beispiel lautet der Dateiname etwa /var/lib/rbldnsd/dnswl/dnswl.magenbrot.net. Das Dateiformat sieht dann so aus:

```
80.12.242.128/28        orange in france is allowed
```

Dies legt liefert jetzt für das komplette Netz 80.12.242.128/28 ein Ergebnis (A- und TXT-Record, reverse).

rbldnsd testen

Das oben verwendete Netz gehört der Firma Orange in Frankreich. Es beheimatet deren SMTP-Server für Kundenmails. Bei einem RBL-Check werden die konfigurierten RBL-Listenserver mit der Reverse-Adresse befragt. Testen kann man das z.B. so:

```
# dig 141.242.12.80.dnswl.magenbrot.net @localhost

; <<>> DiG 9.3.1 <<>> 141.242.12.80.dnswl.magenbrot.net @localhost
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59106
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;141.242.12.80.dnswl.magenbrot.net.        IN A

;; ANSWER SECTION:
141.242.12.80.dnswl.magenbrot.net. 2100 IN A 127.0.0.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jul  6 14:37:24 2009
;; MSG SIZE  rcvd: 72
```

Der TXT-Record dazu wird so abgefragt:

```
# dig 141.242.12.80.dnswl.magenbrot.net @localhost TXT
```

```
; <<>> DiG 9.3.1 <<>> 141.242.12.80.dnswl.magenbrot.net @localhost TXT
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23300
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;141.242.12.80.dnswl.magenbrot.net.        IN TXT

;; ANSWER SECTION:
141.242.12.80.dnswl.magenbrot.net. 2100 IN TXT "orange in france is allowed"

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jul  6 14:43:10 2009
;; MSG SIZE  rcvd: 96
```

Konfiguration des MTA

Postfix

FIXME Achtung, das hier ist noch ungetestet, keine Ahnung ob das so funktioniert!

Blacklist

```
smtpd_client_restrictions = ..., check_client_access dns:maps_rbl, ...

maps_rbl_base = localhost
maps_rbl_lookup = reverse-quad:A
maps_rbl_result = notfound:ignore, 127.0.0.2:ignore, *:deny, ...
```

Whitelist

```
smtpd_client_restrictions = ..., check_client_access dns:maps_rwl, ...

maps_rwl_base = localhost
maps_rwl_lookup = reverse-quad:A
maps_rwl_result = notfound:ignore, 127.0.0.2:ignore, *:ok, ...
```

Sendmail

Blacklist

in /etc/mail/sendmail.mc folgende Zeilen eintragen:

```
FEATURE(`dnsbl',`ix.dnsbl.manitu.net',`"554 Rejected " $&{client_addr} " found in ix.dnsbl.manit
FEATURE(`dnsbl',`sbl-xbl.spamhaus.org',`"554 Rejected " $&{client_addr} " found in sbl-xbl.spamh
```

Whitelist

Für Sendmail muss der folgende m4-Hack in /usr/share/sendmail-cf/feature/dnswl.m4 abgelegt werden:

```
# based IP address white list local
divert(8)
R$*                     $: $&{client_addr}
R::ffff:$-.$-.$-.$-     $: <?> $(host $4.$3.$2.$1._ARG_. $: NotFound $)
```

```
R$-.$-.$-.$-            $: <?> $(host $4.$3.$2.$1._ARG_. $: NotFound $)
R<?>NotFound            $: OKSOFAR
R<?>$+                  $@ <OK>
divert(-1)
```

Jetzt wird folgende Zeile VOR der Konfiguration der DNS-Blacklists eingefügt:

```
dnl whitelist
FEATURE(`dnswl',`localhost')dnl
dnl blacklists
FEATURE(`dnsbl',`ix.dnsbl.manitu.net',`"554 Rejected " $&{client_addr} " found in ix.dnsbl.manit
FEATURE(`dnsbl',`sbl-xbl.spamhaus.org',`"554 Rejected " $&{client_addr} " found in sbl-xbl.spamh
```

Konfiguration von Spamassassin

für Spamassassin wird die local.cf (meist in /etc/mail/spamassassin) mit folgenden Zeilen ergänzt, der Score-Parameter ist nach belieben einzustellen. Soll die DNS-Liste als Blacklist dienen, so ist ein positiver Wert einzutragen, soll die Liste als Whitelist dienen muss ein negativer Wert eingetragen werden.

```
header DNSWL    eval:check_rbl('localDNSWL', 'localhost')
describe DNSWL  local DNS-Whitelisting
score DNSWL     -100
```

POP3 per Telnet testen

Manchmal ist es notwendig die Funktionalität eines Mailservers auf niedrigerer Ebene zu testen, um eventuelle Fehler erkennen zu können. Hier zeige ich, wie man sich per POP3 auf einem Server einloggt, vorhandene Mails auflistet und sich anzeigen lassen kann und welche Kommandos noch so möglich sind.

Benötigt wird dazu ein Telnet-Programm (das telnet-Kommando ist auf den meisten Linux-Boxen vorinstalliert ebenso wie die telnet.exe unter Windows (Ausnahme ist Windows7, hier muss telnet nachinstalliert werden). Alternativ dazu kann man sich unter Windows auf den Putty installieren.

POP3 läuft in den allermeisten Fällen auf TCP Port 110. Die Verbindung kann somit mit folgendem Kommando aufgebaut werden:

```
telnet pop3.mailserver.de 110
```

wenn die Verbindung geklappt hat, meldet sich der POP3-Server etwa so:

```
Connected to pop3.mailserver.de (123.123.123.123).
Escape character is '^]'.
+OK Hello there. <14408.1289900395@localhost.localdomain>
```

Für jedes Kommando, das ihr nun ausführt, antwortet der Server entweder mit einem Fehler und einer optionalen Fehlernummer:

```
-ERR 999 message text
```

oder wenn das Kommando ausgeführt wurde mit:

```
+OK message text
```

Die ersten Kommandos machen Dich mit dem Server bekannt und gewähren Zugriff auf die Mailbox:

```
USER test@mailserver.de
+OK Password required.
PASS test123
+OK logged in.
```

Je nach Mailserver braucht ihr für das Login den Domainteil oder auch nicht. Die Daten hier sind die gleich, die Ihr z.B. auch im Thunderbird eintragen müsst.

Nach dem Login sind folgende Kommandos möglich:

STAT Der Server antwortet hierauf mit: +OK #msgs #bytes
#msgs ist hier die Anzahl der Nachrichten in der Mailbox und #bytes ist die Gesamtgröße aller Nachrichten zusammen.

LIST Dieses Kommando listet alle Mails in der Mailbox auf, eine Mail pro Zeile mit deren Nummer und der Größe in Bytes.

RETR msg# Gibt die Mail mit der Nummer msg# auf dem Display aus.

TOP msg# #lines Dieses Kommando wird nicht von allen Mailservern unterstützt. Es gibt die Header der Mail msg# und die ersten #lines des Bodys aus.

DELE msg# Dieser Befehl markiert die Nachricht msg# zum Löschen. Die Mail wird nicht gelöscht bevor die Verbindung mit QUIT beendet wird. Sollte die Verbindung vor einem QUIT etwa durch einen Timeout beendet werden, sollte der Mailserver die Nachricht nicht löschen.

RSET Alle vorab zum Löschen markierten Mails werden zurückgesetzt, damit ein QUIT diese nicht löscht.

QUIT Entfernt alle zum Löschen markierten Mails und beendet die Verbindung zum Mailserver.

Procmailrc Beispiele

.forward file

```
"|IFS=' '&amp;&amp;exec /full/path/to/procmail -f-||exit 75 #your_login_name"

#    '/full/path/to/' must be replaced with      #
#    the real path such as '/usr/local/bin/'.    #
```

.procmailrc file

```
##########################################################################
#                                                                        #
#   some examples of procmailrc                                          #
#   (c) 1996-1998 Tadashi Kawaguchi &lt;ojin@erehwon.org&gt; #
#   Created on: 5/30/96    Last Modified on: 10/18/98                    #
#                                                                        #
##########################################################################

# Set path #
PATH=/bin:/usr/bin:/usr/local/bin:/opt/local/bin/:$HOME/bin:$HOME:
SENDMAIL=/usr/lib/sendmail
SHELL=/bin/sh
# Set on when debugging #
#VERBOSE=on
VERBOSE=off
# Directory for storing procmail log and rc files
PMDIR=$HOME/.procmail
LOGFILE=$PMDIR/log
# Set environment variables #
UMASK=077
LOCKTIMEOUT=1024
TIMEOUT=960
SUSPEND=16
LINEBUF=4096
# rc files to be included #
INCLUDERC=$PMDIR/rc.sinkspam
INCLUDERC=$PMDIR/rc.autoinfo
INCLUDERC=$PMDIR/rc.autosend
INCLUDERC=$PMDIR/rc.ftpmail
INCLUDERC=$PMDIR/rc.mllist

##############################################################################
#                    forward and aliases                                     #
#   You must change dummy addresses like &quot;your_login_name@your.domain&quot;  #
#   to the real mail address.                                                #
##############################################################################
# forward to your_logname@other.domain
:0
* ^TO.*your_login_name@hostname.domain
! your_logname@other.domain

########################################
#               aliases                #
########################################
:0
* ^TO.*your_login_name@your.domain.*
! your_logname@other.domain

######## aliases for administrator ########
:0
* ^TO.*(P|p|H|h)ostmaster@your.domain.*
! your_logname@other.domain

:0
* ^TO.*mailmaster@your.domain.*
! your_logname@other.domain

:0
* ^TO.*webmaster@your.domain.*
```

```
! your_logname@other.domain

:0
* ^TO.*ftpmaster@your.domain.*
! your_logname@other.domain

:0
* ^TO.*mlmaster@your.domain
! your_logname@other.domain

############ aliases for staff #############
:0
* ^TO.*somebody_1@your.domain.*
! foo@bar.another.domain

########################################
#             other aliases            #
########################################
############ from remote host #############
:0
* ^TO.*your_login_name@host
! your_logname@other.domain

############ from local host ##############
:0
* ^TO.*your_login_name
! your_logname@other.domain

######### `To: foo@someother.domain' ########
:0
* ^Received:.*hostname.domain.*for .(alias-1|alias-2|...|alias-n)@your.domain.*$
! your_logname@other.domain

############ To unknown users #############
:0
* ^Received:.*hostname.domain.*for.*@your.domain.*$
* !^X-Loop: postmaster@your.domain
* !^FROM_DAEMON
{
    TMPFILE=tmp.$$
    TOADDRESS=`formail -uReceived: | formail -xReceived: \
    | sed -e 's/^.*for &lt;//' -e 's/&gt;;.*$//'`

    MAILDIR=$PMDIR/unknown_user

    :0 ac:
    $TMPFILE

    :0 ah
    | (formail -rA &quot;X-Loop: postmaster@your.domain&quot; \
    -I &quot;Precedence: junk&quot; \
    -I &quot;From: postmaster@your.domain&quot; \
    -I &quot;Subject: Returned Mail: Undeliverable&quot; ; \
    echo &quot;The mail you sent could not be delivered to:&quot; ; \
    echo &quot;$TOADDRESS is not a known user.&quot; ; \
    echo &quot;&quot; ; \
    echo &quot;The first 100 lines for the original note follow...&quot; ; \
    echo &quot;&quot; ; \
    head -100 ./$TMPFILE) \
    | $SENDMAIL -oi -t -f'postmaster@your.domain'; \
    rm -f $TMPFILE
}

############ from mailer-daemons #########
:0:
* ^FROM_MAILER
$PMDIR/daemon_mbox

############ trash other junk mails #########
:0
/dev/null
```

auto info

```
########################
#  autoreply info_file  #
```

```
#########################
:0 h
* ^To:.*info@your.domain
| (formail -r -I "From: info@your.domain" \
-I "Reply-To: webmaster@your.domain" \
-I "Subject: your.domain information" \
-I "Errors-To: mailmaster@your.domain" ; \
cat $PMDIR/autoreply/info.txt) | $SENDMAIL -oi -t
```

auto send

```
######################################################################
#    autosend requested one file                                     #
#    This script ignores the body of incoming mails and              #
#    does not return files that have names starting with a dot.      #
#    usage:                                                          #
#        "Subject: send file the_file_you_want"                      #
#        "To: sender@your.domain"                                    #
######################################################################
:0 h
* ^Subject: send file [a-zA-Z0-9_].*
* ^To:.*sender@your.domain
* !^X-Loop: sender@your.domain
* !^Subject:.*Re:
* !^FROM_DAEMON
* !^Subject: send file .*[/.]\.
{
    MAILDIR=$PMDIR/autoreply    # chdir to the autoreply directory

    :0 fhw                # reverse mailheader and extract name
    * ^Subject: send file \/[^ ]*
    | formail -rA "X-Loop: sender@your.domain" \
    -I "From: sender@your.domain"

    FILE="$MATCH"         # the requested filename

    :0 ah
    | cat - ./$FILE | $SENDMAIL -oi -t
}
```

get/put file

```
######################################################################
#                auto get requested one file                         #
#    it ignores the body of incoming mails and does not              #
#    return files that have names starting with a dot                #
#    usage                                                           #
#        "Subject: get file the_file_you_want"                       #
#        "To: geter@your.domain"                                     #
######################################################################
:0 h
* ^To:.*geter@your.domain
* ^Subject: get file [a-zA-Z0-9_].*
* !^X-Loop: geter@your.domain
* !^Subject:.*Re:
* !^FROM_DAEMON
* !^Subject: get file .*[/.]\.
{
    MAILDIR=$PMDIR/ftpmail    # chdir to the archiver directory

    :0 fhw                # reverse mailheader and extract name
    * ^Subject: get file \/[^ ]*
    | formail -rA "X-Loop: geter@your.domain" \
    -I "From: geter@your.domain"

    FILE="$MATCH"             # the requested filename

    :0 ah
    | cat - ./$FILE | $SENDMAIL -oi -t
}

######################################################################
#           auto put requested one file                              #
#    it does not put files that have names                           #
```

```
#    starting with a dot                                          #
#    usage                                                        #
#        "Subject: put file the_file_you_send"                    #
#        "To: puter@your.domain"                                  #
#####################################################################
:0 h
* ^To:.*puter@your.domain
* ^Subject: put file [a-zA-Z0-9_].*
* !^X-Loop: puter@your.domain
* !^Subject:.*Re:
* !^FROM_DAEMON
* !^Subject: put file .*[/.]\.
{
    PUTDIR=$PMDIR/ftpmail
    SUBJECT=`formail -xSubject:`
    FILENAME=`echo "$SUBJECT" | sed -e 's/^.*put file //'`
    REPLYTO=`formail -xFrom:`
    TMPFILE="tmp.$$"

    MAILDIR=$PUTDIR        # chdir to the archiver directory

    :0 fhb
    * ? test ! -f $FILENAME
    | (formail -k -X Content-Type: -X Date: -X From: -X Subject: \
    | cat &gt; $PUTDIR/$FILENAME) ; \
    ls -go &gt; $PUTDIR/allfiles.txt ; \
    touch $PUTDIR/$TMPFILE

    :0 hc
    * ? test ! -f $TMPFILE
    | (formail -A "Precedence: junk" \
    -I "To: $REPLYTO" \
    -I "From: puter@your.domain" \
    -I "Subject: Try again please" \
    -A "X-Loop: puter@your.domain" ; \
    echo "The filename $FILENAME already exists." ; \
    echo "Please try again with another filename." ; \
    echo "" ; echo "----" ; \
    echo "puter@your.domain" ; \
    ) | $SENDMAIL -t

    :0 hc
    * ? test -f $TMPFILE
    | (formail -A "Precedence: junk" \
    -I "To: $REPLYTO" \
    -I "From: puter@your.domain" \
    -I "Subject: Thank you !" \
    -A "X-Loop: puter@your.domain" ; \
    echo "Your mail was saved into a file as follows:" ; \
    echo "" ; \
    ls -go $PUTDIR/$FILENAME ; \
    echo "" ; echo "----" ; \
    echo "puter@your.domain" ; \
    ) | $SENDMAIL -t ; \
    rm -f $PUTDIR/$TMPFILE
}
```

sink spam

```
########################################
#   Sink mails that suspected as Spam   #
########################################

# `From Ô domains on the black list file
BLACKLIST=$PMDIR/banned.domains.txt
FROMDOM=`formail -x'From ' | sed -e 's/.*@//'`
ISBANNED=`grep -i &quot;${FROMDOM}&quot; $BLACKLIST`
:0
* ? test -n &quot;$ISBANNED&quot;
/dev/null

# `From:Ô domains on the black list file
BLACKLIST=$PMDIR/banned.domains.txt
FROMDOM=`formail -x'From:' | sed -e 's/.*@//'`
ISBANNED=`grep -i &quot;${FROMDOM}&quot; $BLACKLIST`
:0
```

```
* ? test -n &quot;$ISBANNED&quot;

/dev/null

# X-Advertisement header found in message
:0
* ^X-Advertisement:.*
/dev/null

# Bogus `To' addresses
:0
* ^TO((F|f)riend|(Y|y)ou|(H|h)ello)@.*
/dev/null

# Spam domains or keywords found in `Received:' header
:0
* ^Received:.*(ybecker.net|earthlink.net|CLOAKED|savetrees).*
/dev/null

# From a numerical userid
:0
* ^From[ :] *[0-9]+@.*
/dev/null

# From a numerical host.domain
:0:
* ^From[ :].*@[0-9]+\.[0-9]+
/dev/null

# Blank Message-Id
:0
* ^Message-Id: *$
/dev/null

# Null Message-Id
:0
* ^Message-Id: <>$
/dev/null
```

maling list

```
##########################################
#             subscribe ml               #
#  add new subscriber to the list file   #
##########################################
:0
* ^To:.*owner-ml@your.domain
* ^Subject:.*(s|S)ubscribe *ml
* !^X-Loop: owner-ml@your.domain
* !^Subject:.*Re:
* !^FROM_DAEMON
{
    WELCOMEFILE=$PMDIR/ml/ml_welcome.txt      # welcome message file
    LISTFILE=$PMDIR/ml/ml.list                # e-mail address file
    TMPFILE=$PMDIR/ml/ml.list.tmp
    FROMADDR=`formail -xFrom:`

    :0 fhw
    * ? test -f $LISTFILE
    | (formail -xFrom: \
    | sed -e 's/^ //' \
      -e '/.*/y/abcdefghijklmnopqrstuvwxyz/ABCDEFGHIJKLMNOPQRSTUVWXYZ/' \
    &gt;&gt; $LISTFILE) ; \
    sort -f $LISTFILE &gt; $TMPFILE ; \
    uniq $TMPFILE &gt; $LISTFILE

    :0 ah
    * ? test -f $TMPFILE
    | (formail -A "Precedence: list" \
    -I "To: $FROMADDR" \
    -I "From: owner-ml@your.domain" \
    -I "Subject: Welcome to our mailing list !" \
    | cat - $WELCOMEFILE 2&gt;&amp;1 | $SENDMAIL -fowner-ml -oi -t) ; \
    rm -f $TMPFILE                      # -f option can be used if you are
                                        # a trusted user, and an alias
                                        # `owner-ml: your_logname, nobody'
```

```
                                        # should exist in /usr/lib/aliases
}

############################################
#               signoff ml                 #
#  remove a subscriber from the list file  #
############################################
:0
* ^To:.*owner-ml@your.domain
* ^Subject:.*(s|S)ignoff *ml
* !^X-Loop: owner-ml@your.domain
* !^Subject:.*Re:
* !^FROM_DAEMON
{
    LEAVEFILE=$PMDIR/ml/ml_leave.txt      # good-bye message file
    LISTFILE=$PMDIR/ml/ml.list
    TMPFILE=$PMDIR/ml/ml.list.tmp
    FROMADDR=`formail -xFrom:`
    OLDADDR=`echo "$FROMADDR" \
    | sed -e '/.*/y/abcdefghijklmnopqrstuvwxyz/ABCDEFGHIJKLMNOPQRSTUVWXYZ/' \
          -e 's/.* <&#047;/' -e 's/>//' -e 's/ (.*)//' -e 's/^ //'`
    DUMMY=`sed -e '/'$OLDADDR'/d' $LISTFILE &gt; $TMPFILE`

    :0 ah
    * ? test -s $TMPFILE
    | (formail -A "Precedence: list" \
    -I "To:$FROMADDR" \
    -I "From: owner-ml@your.domain" \
    -I "Subject: See you again !" \
    | cat - $LEAVEFILE | $SENDMAIL -fowner-ml -oi -t) ; \
    rm -f $LISTFILE ; mv $TMPFILE $LISTFILE
}

##################################
#       send help file           #
##################################
:0
* ^To:.*owner-ml@your.domain
* ^Subject:.*(s|S)end *(h|H)elp.*
* !^X-Loop: owner-ml@your.domain
* !^Subject:.*Re:
* !^FROM_DAEMON
{
    HELPFILE=$PMDIR/ml/ml_help.txt        # help file for the list

    :0 ah
    * ? test -f $HELPFILE
    | formail -rA "X-Loop: owner-ml@your.domain" \
    -A "Precedence: list" \
    -I "From: owner-ml@your.domain" \
    -I "Subject: File: HELP" \
    | cat - $HELPFILE | $SENDMAIL -fowner-ml -oi -t
}

##################################
#        send list file          #
##################################
:0
* ^To:.*owner-ml@your.domain
* ^Subject:.*(s|S)end *(l|L)ist.*
* !^X-Loop: owner-ml@your.domain
* !^Subject:.*Re:
* !^FROM_DAEMON
{
    LISTFILE=$PMDIR/ml/ml.list

    :0 ah
    * ? test -f $LISTFILE
    | formail -rA "X-Loop: owner-ml@your.domain" \
    -A "Precedence: list" \
    -I "From: owner-ml@your.domain" \
    -I "Subject: File: SUBSCRIBER LIST" \
    | cat - $LISTFILE | $SENDMAIL -fowner-ml -oi -t
}

##################################
#       send archive of ML       #
##################################
```

```
:0
* ^To:.*owner-ml@your.domain
* ^Subject:.*(s|S)end *(a|A)rchive.*
* !^X-Loop: owner-ml@your.domain
* !^Subject:.*Re:
* !^FROM_DAEMON
{
    ARCHIVEFILE=$PMDIR/ml/ml_mbox        # archived mbox of the list

    :0 ah
    * ? test -f $ARCHIVEFILE
    | formail -rA "X-Loop: owner-ml@your.domain" \
    -A "Precedence: list" \
    -I "From: owner-ml@your.domain" \
    -I "Subject: File: ML ARCHIVE" \
    | cat - $ARCHIVEFILE | $SENDMAIL -fowner-ml -oi -t
}

##################################
#        Unknown command         #
##################################
:0
* ^To:.*owner-ml@your.domain
* !^X-Loop: owner-ml@your.domain
* !^FROM_DAEMON
{
    HELPFILE=$PMDIR/ml/ml_help.txt
    COMMAND=`formail -xSubject:`

    :0 ah
    * ? test -f $HELPFILE
    | (formail -rA "X-Loop: owner-ml@your.domain" \
    -A "Precedence: list" \
    -I "From: owner-ml@your.domain" \
    -I "Subject: Unknown command" ; \
    echo "&gt; $COMMAND" ; \
    echo "The command you sent was not executable." ; \
    echo "Here is the help for this list." ; \
    echo "" ; \
    cat - $HELPFILE) | $SENDMAIL -fowner-ml -oi -t
}

########################################
#         mailing list                 #
#         initial $NUM = "111000"      #
########################################
:0
* ^To:.*ml@your.domain
* ^Sender: owner-ml@your.domain
/dev/null

:0
* ^To:.*ml@your.domain
* !^X-Loop: ml@your.domain
* !^FROM_DAEMON
{
    LOCKTIMEOUT=2048
    TIMEOUT=1920
    SUSPEND=32
    LINEBUF=20480

    CNTFILE=$PMDIR/ml/ml.num
    LOCKFILE=$CNTFILE$LOCKEXT
    DUMMY=`lockfile -l2048 -s32 $LOCKFILE`  # lock the count file
    NUM=`cat $PMDIR/ml/ml.num`              # get the serial number
    NUM=`echo "$NUM + 1" | /bin/bc`         # then increase it by one
    DUMMY=`echo "$NUM" &gt; $CNTFILE \        # increment the serial number
           &amp;&amp; rm -f $LOCKFILE`             # unlock the count file
                                            # make sure that you have installed
                                            # a 'lockfile' binary which is part
                                            # of the procmail package.
    LISTFILE=$PMDIR/ml/ml.list
    FROMADDR=`formail -xFrom: \
    | sed -e 's/.* <&#047;/' -e 's/>//' -e 's/ (.*)//'`
    SUBJECT=`formail -xSubject:`
    ISMEMBER=`grep -i "${FROMADDR}" $LISTFILE`
    CNT=`echo "$NUM" | sed -e 's/^[1-9][1-9][0-9]//'`
    NSUBJECT=`echo "$SUBJECT" | sed -e 's/^.*[0-9][0-9][0-9]\]//'`
    NSUBJECT="[ml $CNT]$NSUBJECT"          # add list name &amp; serial number
```

```
    :0 hw: $LOCKFILE                        # if not from a subscriber
    * ? test -z "$ISMEMBER"                 # return an error message
    | (formail -r -A "Precedence: junk" \
    -I "From: owner-ml@your.domain" \
    -I "Subject: Re: $SUBJECT - Undeliverable" \
    -A "X-Loop: ml@your.domain" ; \
    echo "The mail you sent could not be delivered." ; \
    echo "Reason: Your are not a subscriber of this list.") \
    | $SENDMAIL -oi -t ; \
    echo "$NUM - 1" | /bin/bc &gt; $CNTFILE   # decrement the serial number

    :0 wc
    * ? test -n "$ISMEMBER"
    | (formail -A "X-Loop: ml@your.domain" \
    -A "Precedence: junk" \
    -I "Reply-To: ml@your.domain" \
    -I "Sender: owner-ml@your.domain" \
    -I "Subject: $NSUBJECT") \
    | $SENDMAIL -fowner-ml `cat $LISTFILE`

    :0 a:             # archive the message shorter than 1000 bytes
    * < 1000
    ml_mbox
}
```

Virenscanner auf dem Client verschluckt STARTTLS

Ich habe für meinen Postfix TLS aktiviert und wollte nun den Thunderbird entsprechend konfigurieren, damit die verschlüsselte Verbindung verwendet wird. Ich habe also im Thunderbird beim SMTP Server die Option TLS aktiviert. Als ich dann versucht habe, über Thunderbird eine Mail über die verschlüsselte Verbindung zu senden, wurde folgende Fehlermeldung angezeigt:

```
Senden der Nachricht fehlgeschlagen.

Fehler beim Senden der Nachricht: Es konnte nicht per STARTTLS mit dem
SMTP-Server mail.magenbrot.net Kontakt aufgenommen werden, da er STARTTLS
nicht in Verbindung mit EHLO unterstützt. Bitte überprüfen bzw.
korrigieren Sie nochmals die Server-Einstellungen.
```

Dieses Problem kann allgemein mit allen möglichen Kombinationen von MTA(Postfix, Sendmail, Exim, Qmail) und Endbenutzerclients wie Thunderbird, Outlook etc. auftreten. Diese Programme verursachen das Problem allerdings nicht, sonder der installierte Virenscanner. In meinem Fall ist das Avast Home Edition (bestätigt wurde das Problem allerdings auch Symantec Antivirus 9). Der Echtzeitscanner lauscht auf Port 25 und leitet ausgehende Mails erstmal durch die Scanengine. Um wohl zu verhindern, dass Thunderbird die Mails verschlüsselt (ein Virenscan wäre dann ja nicht mehr möglich/sinnvoll) wird das Keyword STARTTLS einfach verschluckt.

Zu beachten ist hierbei auch, dass Thunderbird keine Fehlermeldung ausgibt, wenn man in den Einstellungen z.B. „TLS, wenn möglich“ aktiviert hat. Da das „STARTTLS“ nie bei TB ankommt, geht die Software davon aus, dass der Mailserver auch kein TLS unterstützt und übermittelt die Mail unverschlüsselt.

Das Problem ließ sich leider nur lösen, indem ich im Avast das Scannen ausgehender Emails deaktiviert habe.