

SuSE: Plesk & Qmail: Integration von ClamAV (für Suse 9.x)

Achtung! Neu!

Vorher auch folgendes Howto lesen und entscheiden, welcher Weg der bessere für Euch ist:

[HowTo: Spamassassin und ClamAV unter Plesk einbinden](#)

Aus aktuellem Anlass habe ich die u.g. Pakete von Hostbird auch auf diesem Server geparkt:

[Downloads für Plesk / Qmail](#)

(Übersetzung und verbesserte Anleitung von hostbird.com.)

Benötigte Software:

- ClamAV
- qscanq
- [daemontools](#)
- [ripmime](#)

Installation von ripmime

```
#ab ins Source-Verzeichnis
cd /usr/local/src
#runter laden:
wget http://www.pldaniels.com/ripmime/ripmime-1.4.0.3.tar.gz
#auspacken:
tar -xzf ripmime-1.4.0.3.tar.gz
#kompilieren und installieren:
cd ripmime-1.4.0.3/
make
make install
#Symlink ins Verzeichnis /usr/bin/ setzen:
ln -s /usr/local/bin/ripmime /usr/bin/ripmime
```

Installation der daemontools

SuSE: Plesk & Qmail: Integration von ClamAV (für Suse 9.x)

```
#ab ins Source-Verzeichnis
cd /usr/local/src
#runter laden:
wget http://www.hostbird.com/beta/projects/qscanq-psa/daemontools-0.76-2.i386.rpm
#auspacken und installieren:
rpm -Uvh daemontools-0.76-2.i386.rpm
#Autostart setzen:
insserv -d svscan
#Starten:
/etc/init.d/svscan start
```

Hier kommen einige Fehlermeldungen. Die können aber getrost vernachlässigt werden.

(Wer es genau wissen will: Es liegt daran das die daemontools für RedHat/Fedora gedacht sind.)

Installation von qscanq:

```
#ab ins Source-Verzeichnis
cd /usr/local/src
#runter laden:
wget http://www.hostbird.com/beta/projects/qscanq-psa/qscanq-0.43-psa-0.07.tar.gz
#an richtiger Stelle auspacken:
cd /
tar -xzvf /usr/local/src/qscanq-0.43-psa-0.07.tar.gz
#ganz wichtig!!!
cd /usr/local
mv qscanq-0.43-psa-0.07 qscanq-0.43
#für uns:
ln -s qscanq-0.43 qscanq
#sicherheitshalber:
chown root:root -R /usr/local/qscanq-0.43
```

Nun müssen noch die benötigten User und Gruppen angelegt werden:

```
#Gruppen:
groupadd gqscanqg
groupadd gqscanq
#User:
useradd -d /var/qmail/qscanq -g gqscanqg -M -s /bin/true gqscanq
useradd -d /var/qmail/qscanq/log -g gqscanqg -M -s /bin/true gqscanlog
```

Und nun die installations-Routine von qscanq starten:

SuSE: Plesk & Qmail: Integration von ClamAV (für Suse 9.x)

```
#Verzeichnis:  
cd /usr/local/gscanq-0.42  
#install:  
./package/install
```

ClamAV installieren:

Dafür nehmen wir das original SuSE-Paket (evtl. manuell vorher die aktuelle Version suchen!):

```
#ab ins Source-Verzeichnis  
cd /usr/local/src  
#runter laden:  
wget  
ftp://ftp.suse.com/pub/projects/clamav/clamav-0.91.2/9.1-i386/clamav-0.91.2-0.1.i586.rpm  
#auspacken und installieren:  
rpm -ihv clamav-0.91.2-0.1.i586.rpm  
  
#Autostart setzen:  
insserv clamd  
insserv freshclam
```

Nun passen wir noch die Konfiguration an:

In der Datei `/etc/clamav.conf` setzen wir folgende Parameter:

```
#logging aktivieren:  
LogFile /var/log/clamd  
#richtigen User setzen (default: vscan):  
User gqscanq  
#Performance-Schub für viele viele Mails:  
MaxThreads 50
```

In der Datei `/etc/freshclam.conf` müssen folgende Parameter korrigiert werden:

```
#logging aktivieren:  
UpdateLogFile /var/log/freshclam.log  
#richtigen User setzen (default: vscan):  
DatabaseOwner gqscanq
```

Die Logfiles müssen einmal per Hand angelegt werden:

SuSE: Plesk & Qmail: Integration von ClamAV (für Suse 9.x)

```
#Anlegen:
touch /var/log/clamd
touch /var/log/freshclam.log
#Rechte setzen:
chown gqscanq /var/log/clamd
chown gqscanq /var/log/freshclam.log
```

Virus-Datenbank initialisieren und updaten:

```
#Rechte setzen:
chown -R gqscanq /var/lib/clamav/
#Update:
freshclam
```

und ClamAV starten:

```
#ClamAV:
/etc/init.d/clamd start
#regelmässiger Update:
/etc/init.d/freshclam start
```

Installationsfehler?

Beim Blick in `/var/log/clamd` und `/var/log/freshclam` sollten keine Fehler angezeigt werden.

qscanq in Qmail integrieren:

Jetzt wird es aber Zeit, oder?

So wird qmailq in die Qmail-Routine eingehängt:

```
/usr/local/qscanq/command/install-wrap
```

Bei Problemen kann man es einfach deaktivieren:

```
/usr/local/qscanq/command/install-unwrap
```

SuSE: Plesk & Qmail: Integration von ClamAV (für Suse 9.x)

Wichtige Schlußbemerkung!

Selbst verständlich übernehme ich hier keine Garantie!

Vor einem Plesk-Update ist es extrem wichtig den `qscanq` in Qmail zu deaktivieren(!!!) und nach dem Update wieder zu aktivieren.

Beim Update des ClamAV-Paketes ist folgendes zu beachten:

In `/etc/clamav.conf` und `/etc/freshclam.conf` müssen danach die o.g. Änderungen eingepflegt werden. Vorallem der `User qscanq` und `DatabaseOwner qscanq`.

Ein `chown -R qqscanq:qqscanq /var/lib/clamav` ist ebenfalls dringend nötig.

Erst dann können die ClamAV und FreshClam restartet werden. Wenn die Logfiles noch eingeschaltet sind, sollte man auf jedenfall nachsehen, ob noch alles glatt geht.

Getestet auf:

- Ich selbst habe es auf einem 1und1-XXL4-Server mit SuSE 9.1 und Plesk-reloaded getestet.
- Eine weitere Installation erfolgte ohne Probleme auf einem ähnlichen System nur von Schlund&Partner.
- Kommentator Thomas (siehe unten) hat dies auf einem Strato-Server mit SuSE 9.3 nachvollzogen.

Fehlermeldungen:

Neulich passiert: Jede ausgehende Email per `qmail-inject` (also z.B. per `sendmail`) wurde mit einer Fehlermeldung quittiert:

```
qmail-inject: fatal: mail server temporarily rejected message (#4.3.0)
```

Die Lösung war trivial: ClamAV wurde nach dem nächtlichen Update nicht korrekt durchgestartet. Ein Neustart von ClamAV ließ das Mailsystem wieder korrekt arbeiten.

Eindeutige ID: #1068

huschi

2008-01-20 20:40