Heinlein Mailtrace
Logfile-Recherche für Helpdesks

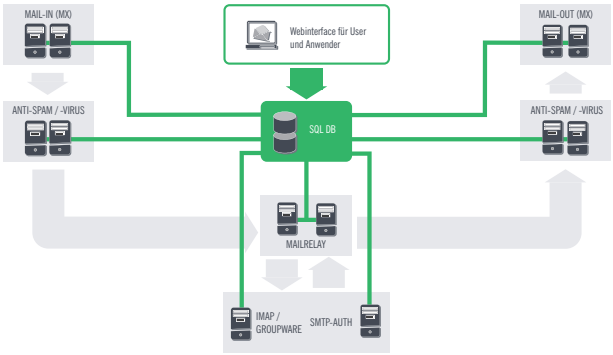
Heinlein Professional Linux Support GmbH
Peer Heinlein p.heinlein@heinlein-support.de

27. Dezember 2012

Zusammenfassung

Sie finden in diesem Admin-Handbuch zu Heinlein Mailtrace das Zusammenspiel aller Komponenten, sowie die nötige Vorgehensweise zum Einrichten von Heinlein Mailtrace erklärt. Handbuch-Version: 2.0 RC3

Inhaltsverzeichnis



1 Heinlein Mailtrace im Überblick

Heinlein Mailtrace analysiert Mail-Logfiles auf beliebig vielen Mailservern und wertet Logzeilen von Postfix, Amavis/SpamAssassin, postgrey und policyd-weight aus. Die Daten werden zusammengefaßt in eine zentrale SQL-Datenbank geschrieben (MySQL, PostgreSQL). Dazu verwendet Heinlein Mailtrace einen Perl-Dämon namens `mailtraced`.

Eine Weboberfläche (PHP/LAMP) ermöglicht die Auswertung der Logfile-Datenbank und bietet Administratoren, Helpdesk-Mitarbeitern und sogar normalen Endanwendern eine schnelle Auswertungssuche, vor allem aber auch eine klare und verständliche Erklärung über den Zustellstatus der jeweiligen E-Mails. Diese Web-GUI wird im folgenden `mailtrace-gui` genannt.

2 Die Installation der RPM-/DEB-Pakete

2.1 Paketinstallation unter SUSE/SLES

Fügen Sie bei SUSE-Systemen dazu einfach unser mailtrace-Repository hinzu und aktualisieren Sie die Paketliste:

```
host:~ # zypper ar -f http://download.opensuse.org/repositories/isv:/heinlein-supp
ort:/mailtrace/SLE\_11\_SP2  Mailtrace

Adding repository 'Mailtrace' [done]
Repository 'Mailtrace' successfully added
Enabled: Yes
Autorefresh: Yes
URI: http://download.opensuse.org/repositories/isv:/heinlein-support:/mailtrace/SLE
\_11\_SP2

host:~ # zypper ref
Repository 'Aktualisierungen für SLES 11 SP2' is up to date.
Retrieving repository 'Mailtrace' metadata [\]

New repository or package signing key received:
Key ID: A39C0B4CF9CA387B
Key Name: isv:heinlein-support OBS Project <isv:heinlein-support@build.opensuse.org>
Key Fingerprint: B2EE8CB9AD6B074AB0F32FBBA39C0B4CF9CA387B
Key Created: Thu Oct 13 15:47:25 2011
Key Expires: Sat Dec 21 14:47:25 2013
Repository: Mailtrace

Do you want to reject the key, trust temporarily, or trust always? [r/t/a/?] (r): a
Retrieving repository 'Mailtrace' metadata [done]
```

Achtung: Wählen Sie die Endung der URL passend zu der von Ihnen eingesetzten Version (`SLE_10_SDK`, `SLE_11`, `SLE_11_SP1`, `SLE_11_SP2`, `openSUSE_11.4`, `openSUSE_12.1`, `openSUSE_12.2`, `openSUSE_Factory`, `openSUSE_Tumbleweed`).

Anschließend können Sie Mailtrace bequem über den Paketmanager mitsamt aller Abhängigkeiten installieren.

Installieren Sie auf dem Webserver das Paket `mailtrace-gui`:

```
host:~ # zypper in mailtrace-gui
```

Und auf den Mailrelays installieren sie `mailtrace-daemon`:

```
host:~ # zypper in mailtrace-daemon
```

Das nächste Kapitel zeigt die weiteren Konfigurationsschritte.

2.2 Paketinstallation unter Debian/Ubuntu

Importieren und überprüfen Sie unter Debian/Ubuntu zunächst den im Repository genutzten Schlüssel. Passen Sie dabei die URL ggf. auf die von Ihnen genutzte Distribution an (`Debian_6.0`, `Debian_5.0`, `xUbuntu_12.04`, `xUbuntu_10.04`):

```
host:~ # wget -O - http://download.opensuse.org/repositories/isv:/heinlein-support:/
mailtrace/Debian_6.0/Release.key | apt-key add -
host:~ # apt-key finger
```

Der Output sollte unseren Schlüssel enthalten:

```
pub   1024D/F9CA387B 2011-10-13 [expires: 2013-12-21]
      Key fingerprint = B2EE 8CB9 AD6B 074A B0F3  2FBB A39C 0B4C F9CA 387B
      uid isv:heinlein-support OBS Project <isv:heinlein-support@build.opensuse.org>
```

Fügen Sie nun das Repository selbst hinzu und aktualisieren Sie die Paketlisten:

```
host:~ # vi /etc/apt/sources.list.d/heinlein-mailtrace.list
deb http://download.opensuse.org/repositories/isv:/heinlein-support:/mailtrace/Debia
n_6.0/ ./
host:~ # apt-get update
```

Sie können nun auf dem Webserver die Mailtrace-GUI installieren...

```
host:~ # apt-get install mailtrace-gui
```

...bzw. auf den Mailrelays den `mailtraced` installieren:

```
host:~ # apt-get install mailtrace-daemon
```

Das nächste Kapitel zeigt die weiteren Konfigurationsschritte.

3 Mailtrace-GUI – Die Weboberfläche zur Auswertung

Beginnen Sie Ihre Mailtrace-Installationen zunächst mit der Installation der Web-GUI, da Sie dort auch bequem alle benötigten Datenbanken und Tabellen anlegen lassen können, in die die `mailtraced`-Dämonen später schreiben werden.

3.1 Konfiguration von URL und Apache-Aliasen

Es entpackt unterhalb von `/opt/heinlein/mailtrace` die PHP-Daten auf Basis eines Zend-Frameworks.

Prüfen und editieren Sie anschließend ggf. das von uns installierte Config-File `/etc/apache2/conf.d/mailtrace`. Dort können Sie über den Alias-Eintrag steuern, unter welcher URI die Weboberfläche später zu erreichen ist.

```
# You might want to set up a virtual host for the server, but it is
# not a requirement. You can as well reach the server under its
# common name under http://www.example.com/mailtrace
#
# NameVirtualHost *
# <VirtualHost *>
#     ServerName mailtrace.example.com
#     DocumentRoot /srv/www/mailtrace.example.com

<IfModule mod_alias.c>
    Alias /mailtrace   /opt/heinlein/mailtrace/frontend/public
</IfModule>

<Directory /opt/heinlein/mailtrace/frontend/public/>
        AllowOverride All
        DirectoryIndex index.php
        Options +FollowSymLinks
</Directory>

# </VirtualHost>
```

Auf Wunsch können Sie Mailtrace ganz analog auch jederzeit als eigenen (virtuellen) Host betreiben.

3.2 Einrichten des Admin-Users

Info: Die Default-Zugangsdaten lauten Username "`admin`" und als Passwort "`admin`".

Die Login-User zur Weboberfläche werden in `/opt/heinlein/mailtrace/frontend/etc/users.ini` definiert.

```
;
;
```

```
; Der benutzte Passwort-Hash wird als {schema} angegeben
; password = "{sha256}sjdjsaskashdkjhasdkja"
; Default ist: {md5}
;
;
; Passwort-Hashes können mit md5sum, sha256sum etc. generiert werden
; echo -n "passwordexample" | sha256sum
;

; Rolle "user" -- Suche limitiert auf die vorgegebenen Mailadressen
;[test]
;roles = mailuser
;emails = dummy@example.com,foo.bar@example.com
;password = f561aaf6ed0bd14d4208bb46a4ccb3ad

; Rolle "helpdesk" -- Suche über alle Daten, aber keine Konfigurationsänderungen erlaubt
;[helpdesk]
;roles = helpdesk
;password = "{sha1}b60d121b438a380c343d5ec3c2037564b82ffef3"

; Rolle "admin" -- Unbeschränkter Zugriff auf Suche und Einstellungen
[admin]
roles = admin
password = "{sha256}8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918"
```

Mailtrace kennt dabei drei verschiedene Rollen:

- `mailuser`
  Ein mailuser kann lediglich die Suchfunktion von Mailtrace benutzen und ist dabei auf die im Attribut ëmails“ gelisteten E-Mail-Adressen beschränkt. Mailtrace stellt sicher, daß eine Suche dieses Users die Liste dieser E-Mailadressen zwangsweise als Suchfilter in ”Mail-Absender“ oder ”Mail-Empfänger“ eingestellt hat.

  Hinweis: Durch einen Bug in der aktuellen Version erscheint das Einstellungsmenü noch in der Navigation, ist vom User aber nicht anwählbar. Der Bug wird alsbald gefixt. In einer der nächsten Versionen können im Attribut `emails` *auch Wildcard-Pattern wie* `*@example.com` *angegeben werden.*

- `helpdesk`
  Ein Account der Rolle `helpdesk` hat eine freie Suchmöglichkeit, jedoch keinen Zugriff auf (Datenbank-) Einstellungen von Mailtrace.

  Hinweis: Durch einen Bug in der aktuellen Version erscheint das Einstellungsmenü noch in der Navigation, ist vom User aber nicht anwählbar. Der Bug wird alsbald gefixt.

- `admin`
  Ein Account der Rolle `admin` hat auch Zugriff auf die Menüpunkte mit Einstellungen, Datenbankpasswörtern oder die Möglichkeit zur Änderung der Erkennungspattern und Erklärungstexte.

Um nicht mit den Default-Zugängen admin/admin öffentlich erreichbar zu sein, sollten Sie jetzt ein neues Admin-Passwort generieren und in die `users.ini` eintragen:

```
echo -n "passwordexample" | sha256sum
```

Falls `sha256sum` bei Ihnen nicht vorhanden ist, nehmen Sie hilfsweise `md5sum`:

```
echo -n "passwordexample" | sha256sum
```

Tragen Sie das Passwort beim Admin-Account ein. Achtung: Das am Ende enthaltene Leerzeichen und Minus-Zeichen gehört *nicht* zum Hash.

Verbinden Sie sich nun mit `http://your.server.name/mailtrace` und loggen Sie sich mit Ihrem `admin`-Account ein.

3.3 Einrichten der Datenbanken

Mailtrace benutzt wahlweise MySQL oder PostgreSQL-Datenbanken um die Logdaten vorzuhalten. Diese müssen nach dem ersten Login in die GUI noch konfiguriert werden.

3.3.1 Datenbankeinrichtung durch den Wizzard

Wenn Mailtrace beim Login einen Fehler in der Datenbankkonfiguration feststellt, wird automatisch ein Datenbank-Wizzard gestartet, der die Einrichtung des Datenbank-Users, der Datenbanken und Tabellen übernimmt.

Tragen Sie dazu in der GUI den SQL-root-User mit dem SQL-root-Passwort ein, anschließend kümmert sich der Wizzard um den ganzen Rest. Wenn alles klappt haben Sie ein fertig benutzbares Mailtrace ohne weitere Nacharbeit.

Selbstverständlich arbeitet Mailtrace nicht mit einem root-Zugang, sondern richtet sich einen User `mailtrace` mit einigen gleichnamigen Datenbanken ein.

Achtung: Merken Sie sich das Datenbank-Kennwort, dass der Wizzard generiert und Ihnen am Ende auch ausgibt. Sie müssen dieses Kennwort noch manuell in der Konfiguration `mailtraced.cfg` der auf den Mailrelays laufenden Mailträce-Dämonen eintragen, damit diese in die Datenbanken schreiben können. Wenn Sie das Datenbank-Passwort einnal verloren haben, können Sie es sich bei den Datenbank-Einstellungen auch im Klartext erneut anzeigen lassen.

Beim ersten Einrichten der Datenbanken muß Mailtrace die aktuellen Erkennungs-Pattern von unserem Server laden. Mailtrace benötigt darum die Möglichkeit eines http/https-Downloads von `update.heinlein-support.de` (IP derzeit: `91.198.250.98`)!

3.3.2 Manuelle Einrichtung der Datenbanken ohne Wizzard

Wenn Sie aus welchen Gründen auch immer den Datenbank-Wizzard nicht benutzen möchten oder können, benötigen Sie einen MySQL oder PostgreSQL-Server, auf dem Sie bereits einen Account für den User `mailtrace` eingerichtet und die drei Datenbanken für `mailtrace` erzeugt haben.

Mailtrace verwendet drei Datenbanken:

1. `mailtrace_logdata`:
   Eine Datenbank für die eigentlichen Logdaten

2. `mailtrace_rules_vendor`:
   Eine Datenbank für die sog. "Vendor-Rules", also die von Heinlein Support bereitgestellten Erkennungsregeln

3. `mailtrace_rules_customer`:
   Eine Datenbank für Ihre hauseigene Erkennungsregeln und Erklärungstexte

Aus diesem Grunde müssen Sie in der Web-GUI *drei* Datenbankzugänge in den Menüpunkten "Datenbank Logdaten" und "Datenbank Erklärungstexte" konfigurieren. Üblicherweise werden Sie bei allen drei Datenbanken absolut identische Zugangsdaten verwenden wollen.

Tipp: Die Datenbank und der benutzte User müssen bereits existieren. Wenn Sie jedoch *Datenbanktabellen erstellen* ankreuzen, richtet sich Mailtrace-GUI alles weitere alleine ein.

Übrigens: Die über die Web-GUI vorgenommenen Datenbankeinstellungen werden in `/opt/heinlein/mailtrace/frontend/etc/HMT/component.ini` gespeichert. Sie sollten diese Datei jedoch nicht manuell editieren.

3.4 SMTP-Relayhost und Absender einrichten

Desweiteren sollten Sie hier noch den Menüpunkt *SMTP-Relayhost* beachten. Sie und Ihre Anwender können später nicht-erkannte SMTP-Meldungen per E-Mail an unseren Mailtrace-Support senden, damit wir die Regelsätze verbessern können. Dazu muß hier ein SMTP-Relayhost und vor allem auch eine Mail-Absenderadresse eingetragen werden.

3.5 `date.timezone` in der `php.ini` beachten

Die Mailtrace-Suche macht umfangreich Gebrauch von Zeit-Berechnungen. Aus diesem Grunde sollten Sie unbedingt darauf achten, dass in PHP Ihre Zeitzone richtig gesetzt ist.

Wenn Sie im `error`-Logfile Ihres Apache-Servers (i.d.R.: `/var/log/apache/error_log` diese Meldung(en) finden...

```
[Fri Jun 01 19:52:06 2012] [error] [client 10.0.40.6] PHP Warning:  date():
It is not safe to rely on the system's timezone settings. You are *required*
to use the date.timezone setting or the date_default_timezone_set()
function. In case you used any of those methods and you are still getting
this warning, you most likely misspelled the timezone identifier. We
selected 'Europe/Berlin' for 'CEST/2.0/DST' instead in
[...]
```

...sollten Sie unbedingt die Zeitzone in der `php.ini` in `/etc/php5/apache2/php.ini` eintragen. In aller Regel wird das die Zeitzone Europe/Berlin sein:

```
;;;;;;;;;;;;;;;;;;
; Module Settings ;
;;;;;;;;;;;;;;;;;;

[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
date.timezone = Europe/Berlin
```

Nach einem Restart sollten die Warnmeldungen im `error`-Logfile beim Ausführen der Suche verschwunden sein.

4 mailtraced – Der Log-Analyser-Dämon

Auf jedem einzelnen Mailrelay, das Sie für die Auswertung berücksichtigen möchten, sollten Sie den Mailtrace-Dämon installieren (RPM-/DEB-Paketname: `mailtrace-daemon`). Er ist in Perl geschrieben und läuft permanent als Dämon im Hintergrund, von wo aus er die Mailserver-Logfiles wie `/var/log/mail` oder `/var/log/mail.*` analysiert.

Um auch für extrem große Setups hochperformant arbeiten zu können, sammelt er die gefundenen Logdaten zunächst lokal im Speicher – er nutzt dafür den separat laufenden Dämon `memcached`

Wenn eine E-Mail das System wieder verlassen hat und der Datensatz komplett ist, wird der komplette Eintrag in einem Write in die zentrale SQL-Datenbank geschrieben. Ist eine Mail auch nach einigen Sekunden noch nicht zugestellt, schreibt der Dämon auch vorzeitig die bereits bekannten Informationen in die SQL-Datenbank, später aktualisiert und ergänzt er dann die bereits angefangenen Datensätze.

Auf diese Art und Weise werden so wenig wie möglich Schreibzugriffe auf die zentrale SQL-Datenbank ausgelöst. Im Idealfall werden pro E-Mail genau zwei Write-Operationen benötigt.

So kann das System auch mit vielen einzelnen Mailrelays und extrem hohem Logaufkommen noch bestmöglichst resourcenschonend arbeiten – und ist entsprechend hochskalierbar. Auch die von Mailtrace genutzte Datenbankstruktur nutzt zahlreiche ausgefallene Kniffe und Optimierungen, um auch über viele Millionen Datensätze noch performant und schnell in Echtzeit Suchergebnisse für Endanwender liefern zu können.

4.1 Installation und Anpassung von logrotate

Verwenden Sie im Idealfall die von uns bereitgestellten Pakete für Debian, Ubuntu, OpenSUSE, SLES, RHEL und andere Distributionen. Sie enthalten bereits alle Bibliotheken und Scripte für `/etc/init.d`. Die Einbindung unseres Repos wurde bereits im vorangegangenen Kapitel gezeigt. Desweiteren sind in den Paketinformationen alle (uns bekannten) Abhängigkeiten zu `memcached`, Perl oder den MySQL/PostgreSQL-Bibliotheken enthalten.

Installieren Sie den Analyser-Dämon auf den Mailservern:

```
host:~ # zypper in mailtrace-daemon
```

Derzeit ist nach Installation der Pakete auf den einzelnen Mailrelays nur noch ein einziger Handgriff manuell durch den Administrator auszuführen.

Nach einem nächtlichen Logrotate-Aufruf muß `mailtraced` einmal neu gestartet werden, da Logrotate /var/log/mail* zusammenpackt und neue, leere Dateien anlegt.

Ergänzen Sie darum Ihren vorhandenen logrotate-Scripte. Diese finden Sie in `/etc/logrotate.d`.

Ändern Sie dort in der Datei `syslog` (bzw. `rsyslog`) die folgende Sektion...

```
/var/log/mail /var/log/mail.info /var/log/mail.warn /var/log/mail.err {
    compress
```

```
    dateext
    maxage 15
    rotate 15
    missingok
    notifempty
    daily
    create 640 root root
    sharedscripts
    postrotate
        /etc/init.d/syslog reload
    endscript
}
```

...und ergänzen Sie dort den postrotate-Aufruf um einen Restart des mailtraced:

```
/var/log/mail /var/log/mail.info /var/log/mail.warn /var/log/mail.err {
    compress
    dateext
    maxage 15
    rotate 15
    missingok
    notifempty
    daily
    create 640 root root
    sharedscripts
    postrotate
        /etc/init.d/syslog reload
        /etc/init.d/mailtraced restart
    endscript
}
```

4.2 Die Config-Datei des Dämons

`mailtraced` zieht seine Informationen aus der Konfigurations-Datei `/etc/mailtrace/mailtraced.cfg`.

Hier müssen sie im Alltrag nur auf drei Punkte achten: Den richtigen Pfad zum Mail-Logfile (`logfile_path`), das zu Ihrem Syslog-Dämon passende Datumsformat (`date_format`) und auf die richtigen Zugangsdaten zu Ihrer SQL-Datenbank. Sie benötigen hier das bei der Einrichtung der Mailtrace-GUI gewählte Passwort für den User `mailtrace`.

```
;
; Achtung: Optionen müssen mit ";" auskommentiert werden, um sie zu deaktivieren.
;
[general]
operational=yes
debug=0
cache_expire_time_seconds=86400
logfile_path=/var/log/mail
logfile_read_idle_time_seconds=3
```

```
; Per Default wird der lokale Hostname für Einträge in der Datenbank genutzt.
; Abweichend kann hier der Hostname manuell gesetzt werden.
;myhostname=localhost

; An verschiedenen Stellen ist es wichtig, welche Domain als lokal angesehen soll.
; Wenn mydomain nicht gesetzt ist, wird der Wert aus "postconf mydomain" ausgelesen.
; Feature vorbereitet -- wird erst in späteren Releases relevant werden
; mydomain=example.com

; Zeit in Sekunden, nach den der Dämon als aktiv gewertet werden soll
keep_alive_seconds=30

; Format der Zeitangabe im mail-Logfile:
; classic (Jul 12 10:53:25 host service)
; modern  (2011-07-12T10:47:21.662587+02:00 host service)
date_format=classic

; Mit diesen Optionen können "verify"-Anfragen von Postfix von der Erfassung
; ausgenommen werden. "address_verify" von Postfix nutzen, sollten Sie hier den
; Wert von "address_verify_sender" eintragen. Mails dieses Absenders werden dann von
; alle Hosts unterhalb von mydomain ignoriert.
ignore_verify_log_entries=yes
ignore_connects_from=verify

[database]
; dbtype=PostgreSQL
; dbport=5432
dbtype=MySQL
dbport=3306
;
dbhost=localhost
dbname=mailtrace_logdata
dbuser=mailtrace
dbpassword=xxxxxxxxxxxxxxx
;
db_disconnect_sleeptime_seconds=9
db_disk_full_sleeptime_seconds=3600
;db_max_age=21
```

4.3 Der erste Start des mailtraced

Beim ersten Start beginnt `mailtraced` das Mail-Logfile in voller Länge einzulesen und zu analysieren. Wundern Sie sich also nicht, wenn der Dämon zunächst fleißig arbeitet und auch in `top` & Co mit einer entsprechend hohen CPU-Auslastung zu sehen ist.

Sobald der Dämon das Ende des Logfiles erreicht hat wird die Last nachlasssen, da er dann nur noch die jeweils neu eintreffenden Logzeilen abgreifen und verarbeiten muß.

Direkt nach dem Start des `mailtraced` sollten Sie bereits in der Web-GUI die ersten erfaßten Logdaten finden. Führen Sie einfach eine leere Suche aus, sie sollten dann bereits Ergebnisse sehen.

4.4 Troubleshooting und Aufrufparameter

Der Dämon kennt einige Aufrufparameter, die Sie auch jederzeit über `mailtraced -h` einsehen können:

```
host:~ # mailtraced  -h
mailtraced <OPTIONS>

   --debug               Start mailtraced in debugging modus (more verbose in syslog)
   --full-debug          Redirected every output of perl to /root/mailtraced.debug
                         BE CAREFUL: This file could grow very fast!
   --expire=seconds      Define after which amount of seconds the cached data
                         should be discarded
   --nofollow            Stop the daemon if end of file is reached
   --clean               Trigger the clean function (database cleanup)
   --max-age=N           Delete entries older than N days from now. Works only
                         in combination with --clean
   --benchmark           Print the duration of daemon runtime to syslog. Only
                         reasonable with the --nofollow option
   --help                Print this text
   --idle=seconds        Define the idle time before retrying to fetch new lines when
                         the end of logfile is reached
   --logfile=path        Specify the logfile which should be analysed
   --monitoring=<string> Define an string for monitoring output behaviour:
                         s: Daemon status (running, not running)
                         b: Print out backlog time (difference between workstatus
                         and current time in seconds)
   --pid=pidfile         Define an alternative pidfile (default is
                         /var/run/mailtraced.pid)

PLEASE NOTE: Define options in /etc/mailtrace/mailtraced.conf!
```

Diese Parameter sind für Debugging-Zwecke oder Sonderfälle gedacht, beispielsweise, wenn große Mengen bereits wegrotierter alter Mail-Logdaten nachträglich eingelesen werden sollen.

Sollte `mailtraced` Ihre Logdaten nicht richtig finden oder verarbeiten, können Sie über `--debug` und `--full-debug` weitere Informationen abgreifen.

5 Wartungsarbeiten im laufenden Betrieb

Mailtrace wird im täglichen Betrieb seine Datenbanken kontinuierlich füllen und weiter anwachsen. Um Platz zu schaffen – aber auch um den datenschutzrechtlichen Vorschriften gerecht zu werden – müssen Sie von Zeit zu Zeit die veralteten Einträge ablöschen lassen.

Diese Aufgabe kann ein beliebiger `mailtraced` ihres Pools übernehmen. Wird er mit den Aufrufparametern `--clean` gestartet, so liest er aus der Mailtrace-SQL-Datenbank die maximale Haltezeit aus, die Sie im Webinterface eingestellt hatten. Anschließend kümmert sich dieser `mailtrace` um das Ablöschen der Daten.

Beim clean-Parameter verbleibt `mailtraced` nicht als Dämon im Speicher, sondern erledigt die Aufräumarbeit und beendet sich dann wieder kommentarlos.

Sie können diesen Aufruf also problemlos parallel zu einem als Dämon mitlaufenden ëchten“ `mailtraced` vornehmen. Dieser wird davon nicht gestört. Sie sollten einen entsprechenden Aufruf in Ihre Crontab eintragen, damit beispielsweise einmal in der Nacht aufgeräumt wird und Sie regelmäßig wieder Platz in der Datenbank schaffen.

Achtung: Die von uns ausgelieferten RPM-/Debian-Pakete haben dazu bereits einen passenden Eintrag in `/etc/cron.daily/mailtraced`! Sie müssen sich hier also um nichts mehr kümmern...

Übrigens: Wenn Sie `mailtraced` auf mehreren Servern installiert haben, ist es unkritisch, wenn bei gleicher Konfiguration im Cluster mehrere `mailtraced` einen Aufräumjob starten. Der erste `mailtraced` erledigt den Job – die anderen Prozesse haben nichts mehr zu tun und werden entsprechend schnell ergebnislos fertig sein.

Ergänzend können Sie einem `mailtraced` auch über den weiteren Aurrufparameter `--max-age=<n>` vorgeben, wie lange die maximale Haltezeit sein soll. Der `mailtraced` wird dann denn zentralen Konfigurationswert aus der Datenbank ignorieren und sich stattdessen nach dem per Parameter übergebenen Wert richten:

```
host:~ # mailtraced  --max-age=5 --clean
```

Abbildung 1: Mailtrace - Suchmaske

6 Mailtrace in der Bedienung

6.1 Die Suchmaske

Nachfolgend wird die Suchmaske von Mailtrace näher erläutert, damit Sie schnell in der Lage sind die Informationen zu finden, die Sie suchen.

6.1.1 Standard-Suchoptionen

1. **Absender** - Tragen Sie in diesem Feld den bereits bekannten Absender der gesuchten E-Mail ein.
2. **Empfänger** - Tragen Sie in diesem Feld den bereits bekannten Empfänger der gesuchen E-Mail ein.
3. **Zeitraum** - Wählen Sie unter dieser Option bitte die Zeitspanne, in welcher Sie die Verarbeitung der gesuchten E-Mail vermuten. Der angegebene Zeitraum gilt für die Einlieferung, sowie für die Auslieferung der gesuchten E-Mail.
4. **Message-ID** - Jede E-Mail hat eine ihr eigene Message-ID, anhand derer sie sicher in den Logfiles wiedergefunden werden kann.

Warnung: Verwechseln Sie die Message-ID nicht mit der Queue-ID. Die Queue-ID dient nur zur internen Identifizierung im System und wird auch nicht im Header der E-Mail hinterlegt.

5. **Status** - Jede im System befindliche E-Mail besitzt einen bestimmten Status, nach welchem unter diesem Punkt gesucht werden kann. Folgende Status sind möglich:
   - **Gesendet** - Bedeutet, dass die E-Mail das System ordnungsgemäß verlassen hat und an einen anderen Server übergeben wurde.

Abbildung 2: Mailtrace - Suchmaske (Erweitertert)

- **Deferred** - Sagt aus, dass eine E-Mail sich noch im überwachten Mailsystem befindet. Dies kann verschiedene Gründe haben. Generell besitzt eine E-Mail den Status **deferred**, wenn die versuchte Zustellung von der Gegenseite mit einem 4XX-Fehler zunächst abgelehnt wurde.
- **Bounced** - Wenn eine E-Mail sich bereits im Mailsystem befindet und intern ein Fehler auftritt, welcher die Zustellung der betreffenden E-Mail unmöglich macht, erzeugt das Mailsystem eine sog. Bounce-Meldung mit dem Grund für die Unzustellbarkeit. Diese Suchoption findet Log-Einträge von E-Mails, die im überwachten System eine solche Bounce-Meldung ausgelöst haben.
- **Rejected** - Ebenso wie ein Bounce, tritt ein **Reject** bei Unzustellbarkeit einer E-Mail auf. Im Falle des überwachten Systems betrifft dies hauptsächlich Zustellungsversuche auf entfernte Systeme, welche mit einer bestimmten Reject-Meldung die Annahme der E-Mail verweigert haben.
- **Unbekannt** - Zwischen der Annahme einer E-Mail und dessen Auslieferung bzw. dessen Auslieferungsversuch, kann je nach vorliegendem System eine bestimmte Zeitspanne bestehen. In diesem Zeitraum besteht zwar ein Logeintrag zur Einlieferung, aber noch kein Logeintrag zur (versuchten) Auslieferung. Befindet sich eine E-Mail in diesem Status, ist dieser Unbekannt.

6.1.2 Erweiterte Suchoptionen

1. **Status-Meldung** - Zusätzlich zum Status gibt der Server, welcher die E-Mails annimmt, eine Texterklärung bezüglich des übermittelten Status-Codes aus. Unter dieser Suchoption können Sie nach gewünschten Wortlauten einer Statusmeldung suchen.

2. **Client (Hostname/IP)** - Der einliefernde Mailserver besitzt immer eine IP-Adresse und bei einem korrekten DNS-Setup einen zugehörigen auflösbaren Hostnamen. Unter dieser Suchoption können Sie direkt nach dieser IP-Adresse oder dem zugeordneten DNS-Hostnamen suchen.

3. **Empfangsserver (Hostname/IP)** - Diese Option beschreibt den Server, an welchen die Mail weitergegeben werden soll. Auch an dieser Stelle kann nach dem Hostname gesucht werden, welcher über DNS zurück gegeben wird.

4. **Meldender Server** - Hiermit ist der Server gemeint, auf welchem einer der Mailtrace Collector-Daemons installiert ist. Jeder der eingerichteten Server ist an dieser Stelle über eine Drop-Down-Box anwählbar. Erscheint ein gesuchter Server nicht in dieser Liste, existiert in der Datenbank kein Logeintrag für diesen Server.

5. **Queue-ID** - Die Queue-ID dient der internen Identifizierung einer E-Mail. Sie wird nicht in den Header geschrieben bzw. außerhalb des Systems verwendet. Sobald ein Server eine E-Mail angenommen hat, wird die Queue-ID über den SMTP-Dialog im Zusammenhang mit einer 2XX-Bestätigung bekanntgegeben.

6.2 Auswertung der Suchergebnisse

Nachdem die Suche ausgeführt wurde, erscheint eine Auflistung der Suchergebnisse in einer Box unterhalb der Suchmaske. Bei der Anzeige werden nur die notwendigsten Informationen herangezogen. Diese umfassen folgende Werte:

1. **Die Zeit der Einlieferung der E-Mail** - Eine E-Mail besitzt zwei Zeiten innerhalb der Mailtrace-Datenbank. Zum einen die Zeit der Einlieferung und zum anderen die Zeit der Auslieferung. Im Ergebnisbereich der Suche wird die Zeit der Auslieferung angezeigt.

2. **Der Absender und Empfänger der E-Mail** - Im Bereich der Suchergebnisse werden Absender und Empfänger ausgegeben, welche durch einen Pfeil identifiziert werden können. Somit handelt es sich bei der linken E-Mailadresse um den Absender und bei der rechten E-Mailadresse um den Empfänger.

3. **Die Message-ID der E-Mail** - Die Message-ID dient zur Identifizierung einer E-Mail.

4. **Die Status-Meldung des Mailservers** - An dieser Stelle wird in Kurzform der aktuelle Status der betreffenden E-Mail ausgegeben. Welche Statusmeldungen generell existieren wurde bereits erläutert. Für die Übersicht der Suchergebnisse existieren nur vier verschiedene Status, um eine bessere Übersicht zu gewährleisten.

    - Nachricht erfolgreich versendet
    - Nachricht noch nicht versendet
    - Nachricht zurückgewiesen
    - Status unbekannt

6.3 Die Detailansicht

Neben der verkürzten Übersicht existiert eine detaillierte Übersicht für das jeweilige Suchergebnis. Sie zeigt den genauen Verlauf der betreffenden E-Mail durch das überwachte Mailsystem. Dieser Verlauf umfasst die Einlieferung der E-Mail, ihr Weg durch die Spamfilterung bis zur engültigen Auslieferung.

Demnach versteht sich die detaillierte Übersicht als eine Zusammenfassung aller vorhandenen Datenbankeinträge der betreffenden E-Mail. Da aber auch an dieser Stelle nicht alle vorliegenden Informationen aus Platzgründen angezeigt werden können, werden zwei Buttons zur Verfügung gestellt, Details und Erklärung.

Der Details-Button für den jeweiligen Eintrag öffnet ein neues Fenster, in welchem alle vorliegenden Informationen des Eintrags in einer Komplett-Übersicht ausgegeben werden. Eine Erläuterung des Buttons zur Anzeige einer Erklärung folgt im nachfolgenden Abschnitt.

6.4 Anzeigen einer leicht verständlichen Erklärung

Mailtrace ist dafür entwickelt worden, 1st-Level Supportern bei ihrer täglichen Arbeit zu unterstützen. Darüber hinaus wird auch den einzelnen E-Mail Nutzern die Möglichkeit gegeben, den Verbleib ihrer E-Mails eigenständig zu recherchieren. Diese verfügen in der Regel über kein tiefgreifendes technisches Wissen und können durch die angezeigten Suchresultate schnell überfordert sein.

Aus diesem Grund stellt Mailtrace einen Button zur Anzeige einer leicht verständlichen Erklärung bereit. Wird dieser gedrückt, öffnet sich ein neues Fenster welches die Erklärung in reiner Textform beinhaltet. 1st-Level Supporter haben hierdurch zudem die Möglichkeit dem anfragenden Kunden, relevante Informationen in Kurzform verständlich zu vermitteln.

7 Credits und Changelog

In Mailtrace stecken schon jetzt über fünf Mannjahre Entwicklungsarbeit. Insb. die ausgefallene und hochperformante Datenbankstruktur hat erhebliche Entwicklungszeit gekostet.

7.1 Status quo

- Mailtrace 2.0 RC3 befindet sich im Kundeneinsatz. Automatische Regelupdates und fertige Installationspakete sind vorhanden.
- Die Unterstützung für PostgreSQL und SQLite sind vorhanden und sollten gehen, aber nur MySQL ist umfassend getestet.

7.2 Known Bugs

- In der ausgeklappten Ansicht eines Suchtreffers unterscheiden Graphik und Texte bei abgelehnten E-Mails noch nicht richtig zwischen ein- und ausgehenden E-Mails. Haken/Kreuze werden ggf. noch doppelt dargestellt, der Status-Text ist etwas schwammig/mißverständlich.
- In bestimmten Situationen werden Reject-Gründe von policyd-weight noch nicht richtig erfaßt.
- Bei den Rollen üseründ "helpdesk"wird noch das Einstellungs-Menü eingeblendet (kann aber korrekterweise nicht benutzt werden)
- Layout- und Darstellungsfehler in diesem Handbuch :-)
- Wenn weniger als 10 Ergebnisse am aktuellen Tag gefunden werden, wird nicht automatisch am Vortrag ergänzend gesucht
- Blättern in den Suchergebnissen wirft teilweise noch Layout durcheinander
- PostgreSQL-Import der Erklärungstexte wirft Boolean-Fehler und verliert Einträge, MySQL geht aber
- mailtraced wirft im Debug-Modus noch md5sum-Fehler, ist aber total in Ordnung

7.3 Roadmap

- Verbesserung der Erkennungsregeln und Erklärungstexte ("Vendor Rules"). Diese werden über Regel-Updates von Heinlein Support ständig aktualisiert bereitgestellt.
- Ein Login von Endusern bei gleichzeitiger Authentifizierung an einer zentralen SQL-DB, einem LDAP- oder einem AD-Server. Jeder User sieht dabei stets nur seine eigenen E-Mails.
- Die Möglichkeit des Versandes von E-Mail-Status-Reports direkt an Absender oder Empfänger der E-Mail. So kann ein Helpdesk Antworten direkt aus der Mailtrace-GUI heraus versenden.

- Mailtrace wird auch den Verlauf einer E-Mail über mehrere Server hinweg zusammengefaßt anzeigen können. Dazu muß die Darstellungsweise in den Suchtreffern noch überarbeitet werden.

7.4 Credits

Die folgenden Kollegen von Heinlein Support haben an Mailtrace maßgeblich mitgewirkt:

- Christoph Graupner: Mailtrace-GUI, Suchalgorithmen, Datenbankdesign/-optimierung
- Stefan Neben: `mailtraced`-Dämon
- Henri Schmidt: Mailtrace-GUI, Bugfixing, Design
- Daniel Mohn: `mailtraced`-Dämon, Datenbank-Wizzard
- Philipp Mühlmeister (extern): Usability und Design
- Peer Heinlein: Idee, Konzept, Proof-of-Concept, Handbuch, Erklärungstexte

Herzlichen Dank an diese und alle anderen, die im Laufe der Zeit beteiligt waren!

8 Lizenzhinweise

Mailtrace basiert teilweise auf GPL-lizensierter Software.

Mailtrace unterliegt einer kommerziellen Lizenz der Heinlein Professional Linux Support GmbH ("Heinlein Support"). Ein Einsatz von Mailtrace erfordert eine Lizensierung von Heinlein Support. Wenden Sie sich dazu an `mail@heinlein-support.de`.