Unterschiede Postfix 1.1.x zu Postfix 2.4

Ralf Hildebrandt

T-Systems Business Services

Berlin, 30. März 2006

Inhalt

Das Entwicklungsmodell

- “stable”-Version wird ab und an veröffentlicht
- “snapshot”-Version enthält neue Features die in die nächste “stable” einfließen (oder auch nicht)

Das Entwicklungsmodell II

- keine Bananenware:
  Stabil genug für den täglichen Gebrauch

Postfix 2.0

Postfix 2.0 (22.12.2002)

virtual domains

- `virtual_maps` wird zu `virtual_alias_maps` und `virtual_alias_domains`
- `virtual_mailbox_maps` und `virtual_mailbox_domains`

MIME Unterstützung

- Postfix hat echte MIME-Unterstützung
- `header_checks` erkennen MIME-Header in Anhängen
- drei Klassen von `header`-checks:
  - `header_checks` – for primary message headers except MIME headers
  - `mime_header_checks` – for MIME headers
  - `nested_header_checks` – for headers of attached email messages except MIME headers

Kürzung von zu langen Zeilen

- Postfixs `smtp` Client bricht Zeilen, die länger als `smtp_line_length_limit` (standardmäßig: 990) sind um.
  Ältere Postfix Version taten dies bei `line_length_limit` Zeichen (standardmäßig: 2048).

Adreßklassen

- Adressenklassen für `local`, `virtual`, `relay`, `smtp`
- `relay`-Transport für Mail von außen nach innen

Änderungen in den `smtpd_*_restrictions`

- `reject_maps_rbl` wird abgelöst durch `reject_rbl_client`
- `reject_rhsbl_sender rbl.domain.tld` ist neu
- `rbl_reply_maps` erlaubt individuelle Antworten je nach RBL

Änderungen an Maps

- In `smtpd`-maps benutzt Postfix nun `<>` für die leere Adresse um Fehler in einigen Berkeley DB Implementierungen zu umgehen
- `user@domain` funktioniert nun in `transport_maps`
- neue Aktion `HOLD`

Selektives Filtern

- Selektives Filtern mit `FILTER transport:nexthop` in `header-/body_checks` und `smtpd_*_restrictions`

Dies und das

- `X-Original-To:` Header
- `proxy_interfaces` Parameter für Mailserver hinter NAT.
- Warnung bei Gebrauch einer Domain in `mydestination` und einer virtuellen Domain.
- LDAP API v1 wird nicht länger unterstützt
- Warnungen des Queuemanagers bei “Verstopfung”
- Performanceverbesserungen
- Änderungen im Logging

Postfix 2.1

Postfix 2.1 (22.04.2004)

Neue Daemonen

- neue Daemonen `trace` und `verify`
- `nqmgr` wird zum `qmgr`, `qmgr` wird `oqmgr`

Änderungen in den smtpd_*_restrictions

- RBLs mit verschiedenen Rückgabewerten: `reject_rbl_client zen.spamhaus.org=127.0.0.4` weist Client ab, die in `zen.spamhaus.org` mit einem `127.0.0.4` Adreßeintrag gelistet sind.
- `check_*_ns_access` und check_*_mx_access kontrollieren den Zugriff nach NS und MX Eintrag eines Hostnamen oder einer Domain.

Neues in Maps

- CIDR Maps
- Negierung (`!/pattern/`) in PCRE Maps
- `WARN text...`
- `PREPEND headername: headervalue`
- `REDIRECT user@domain`

Überprüfung des Absenders

- Nicht-existente Absenderadressen für Domain der Klassen local, virtual oder relay domain können abgewiesen werden:
  `reject_unlisted_sender=yes`.
- Prüfung des Absenders gegen die Authorisierungsinformationen:
  - `reject_unauth_sender_login_mismatch`
  - `reject_auth_sender_login_mismatch`
  - `sender_login_maps`
- `reject_unverified_sender` prüft bei zuständigen Server, ob die Absenderadresse akzeptiert wird.

Neue Filtermöglichkeiten

- `smtpd_proxy_filter` kann Mail filtern bevor die Annahme quittiert wird
- `receive_override_options` erlaubt es, die Adressumschreibung und Prüfung auf unbekannte Nutzer vor und hinter den Filter zu verteilen
- Policy Delegierung an ein externes Programm

Erweiterungen des SMTP Protokolls

- `xclient` Support
  zur Prüfung von Zugriffsmechanismen
- `XFORWARD addr=client-address name=client-hostname`
  zur Übermittlung des originalen Clients an einen `content_filter`

Dies und das

- bcc in Abhängigkeit vom Absender oder Empfänger
- `sendmail -bv`: Postfix “versucht” die Zustellung, ohne sie durchzuführen
- `user@1.2.3.4` ist nicht mehr erlaubt, nur noch `user@[1.2.3.4]`
- `bounce_queue_lifetime` steuert die Lebensdauer von Bounces
- LDAP/mySQL Verbesserungen
- `NOQUEUE` bei Abweisungen, da kein Queuefile mehr erzeugt wurde.

Postfix 2.2

Postfix 2.2 (09.03.2005)

TLS und IPv6

- TLS und IPv6 sind nun integriert

Adressumschreibung

- Postfix schreibt Header in Mails von Clients nicht mehr um
- `smtp_generic_maps` - wenn Mail per SMTP das eigene Netz verläßt, werden Adressen umgeschrieben
- `canonical_maps` werden feiner kontrolliert durch `canonical_classes` bzw. `sender_canonical_classes` und `recipient_canonical_classes`, wobei man die folgenden Sachen umschreiben kann:
  - `envelope_sender`
  - `header_sender`
  - `envelope_recipient`
  - `header_recipient`

Verbesserungen in Maps

- `CDB`, `SDBM` und `NIS+` werden als Maps unterstützt
- Freiform SQL Abfragen und Domainfilter für LDAP, MySQL und PostgreSQL
- `REPLACE` in `header-` und `body_checks`

Sicherheit

- Beschränkung der Transaktionen eines Client pro Zeiteinheit (`anvil`)
- `authorized_submit_users` bestimmt welche lokalen User Mail einliefern dürfen
- Selektives Abschalten von ESMTP Fähigkeiten wie `AUTH` oder `STARTTLS` in `smtp` und `smtpd`

Performance

- Wiederverwendung von bestehenden Verbindungen durch `smtp`
- Neuer Daemon `discard` zum Wegschmeissen von Mail
- gehashte Queueverzeichnisse (`deferred` und `defer`)

Postfix 2.3

Postfix 2.3 (11.07.2006)

Unterstützung von DSN gem. RFC 3461-3464

Hiermit kann eine Quittierung der erfolgreichen (oder erfolglosen) Auslieferung vom Absender angefordert werden. Es gibt mehrere Reportklassen:

- `failure`, wenn eine Benachrichtigung bei Zustellproblemen erzeugt werden soll,
- `delay` für eine Benachrichtigung bei Zustellverzögerungen und
- `success`, für Benachrichtigung erfolgreicher Zustellung.

User Agents mit DSN Unterstützung sind z.B. elm-2.4ME+31 und mutt.

Lustige Anwendungen

Damit kann man z.B. bei manchen Systemen sehen, wohin `postmaster@example.com` zugestellt wird!

Oha!

/dev/null

Vorlagen-gesteuerte DSN-Nachrichten

Seit snapshot-20051113 bietet Postfix vorlagen-gesteuerte DSN-Meldungen und kann somit nun auch deutsch-sprachige Statusmeldungen erstellen:

`http://postfix.state-of-mind.de/bounce-templates`

Wann werden diese eingesetzt?

Eine Zustell-Status-Nachricht wird immer dann generiert und an den Absender gesendet, wenn:

- ein Fehler bei der Zustellung aufgetreten ist
- eine Verzögerung bei der Zustellung auftritt
- eine Zustell-Bestätigung angefordert wurde
- eine Empfänger-Adressen-Bestätigung angefordert wurde

“enhanced status codes” (RFC 3463)

In Maps (siehe `access(5)`) kann man nun:

```
REJECT 5.7.1 You can't go here from there
```

angeben was dann hoffentlich vom MUA (Outlook, Mozilla, etc.) in eine luser-verständliche Fehlermeldung umgewandelt wird.
In unserem Beispiel laut RFC:
“Delivery not authorized, message refused” – The sender is not authorized to send to the destination.

Detaillierteres Logging

`delay=n` wurde zu `delay=n, delays=a/b/c/d`, wobei:

- `a`: Zeit vor dem `qmgr`, einschließlich der Übertragungszeit
- `b`: Zeit innerhalb des `qmgr`
- `c`: Zeit für Verbindungsaufbau, inkl. DNS, HELO und TLS-Handshake
- `d`: Übertragungsdauer

Alle Zeitangaben sind jetzt endlich genauer als 1s!

Detaillierteres Logging II

- `conn_use=n`
  zeigt die Anzahl der Wiederverwendungen der Verbindung
- `relay=hostname[ip.add.re.ss]:port`
  zeigt nun auch den Port an, der kontaktiert wurde

Beispiel

Von `mail.charite.de`:

```
Feb  1 15:13:49 mail postfix/smtp[14123]: 94A06221600:
to=<recipient@charite.de>,
relay=127.0.0.1[127.0.0.1]:10025, conn_use=2, ...
```

- `relay=127.0.0.1[127.0.0.1]:10025`
  wir reden mit `amavisd-new`
- `conn_use=2`
  das passiert wohl öfter

Beispiel II

```
... delay=3.4, delays=2.8/0.05/0/0.56, dsn=2.6.0, status=sent
(250 2.6.0 Ok, id=15344-04-2, from MTA([127.0.0.1]:10026):
250 2.0.0 Ok: queued as AEC2222155B)
```

- `delay=3.4, delays=2.8/0.05/0/0.56`
  am längsten dauerte die Übertragung (Zeit vor dem `qmgr`, einschließlich der Übertragungszeit)

Absenderabhängiger relayhost

Für den Heimbenutzer – in Abhängigkeit der Absenderadresse wählt Postfix den passenden relayhost sowie die dazugehörigen SMTP-AUTH Benutrzer und Passwort:

```
sender_dependent_relayhost_maps =
   hash:/etc/postfix/sender_relay
smtp_sasl_password_maps =
   hash:/etc/postfix/smtp_passwords
smtp_sender_dependent_authentication = yes
```

Beispiel: Absenderabhängiger relayhost

/etc/postfix/sender_relay enthält:

```
ralf@gmx.de          smtp.gmx.de
constanze@web.de     smtp.web.de
```

und in /etc/postfix/smtp_passwords:

```
ralf@gmx.de          ralf:ralfpass
constanze@web.de     constanze:constanzepass
```

Aber Vorsicht!

Dies deaktiviert natürlich das Connection Caching im `smtp`-Client!

Gemeinsamer Code für LMTP- und SMTP-Clients

Der `smtp`-Client implementiert nun sowohl das (E)SMTP- als auch das LMTP-Protokoll.
Dadurch werden viele `lmtp_*`-Parameter eingeführt, die zuvor nur aus dem `smtp_*`-Kontext bekannt waren.

Every ten years I do. . .

Wietse will nicht ewig an Postfix arbeiten:

> “Every ten years I do something completely different”

Daher werden jetzt zahlreiche “plugin”-Möglichkeiten innerhalb von Postfix geschaffen.

. . . something completely different

Authentifizierungs-Plugins

Unterstützung unterschiedlicher Authentifizierungs-Frameworks im kombinierten `(s|l)mtp`-Client und `smtpd`-Server

- Cyrus-SASL
- Dovecot-SASL

Cyrus-SASL – problematisch: keine Doku, niemand versteht es...

- Lutz Jaenickes Patch hatte kleinere Fehler und Inkonsistenzen, die ausgemerzt wurden
- neuer per-site TLS policy-Mechanismus, der besser gegen DNS-Spoofing Attacken schützt
- Generell: viele Verbesserungen bei TLS

Begrenzung der Anzahl von neuen TLS Sitzungen pro Zeiteinheit

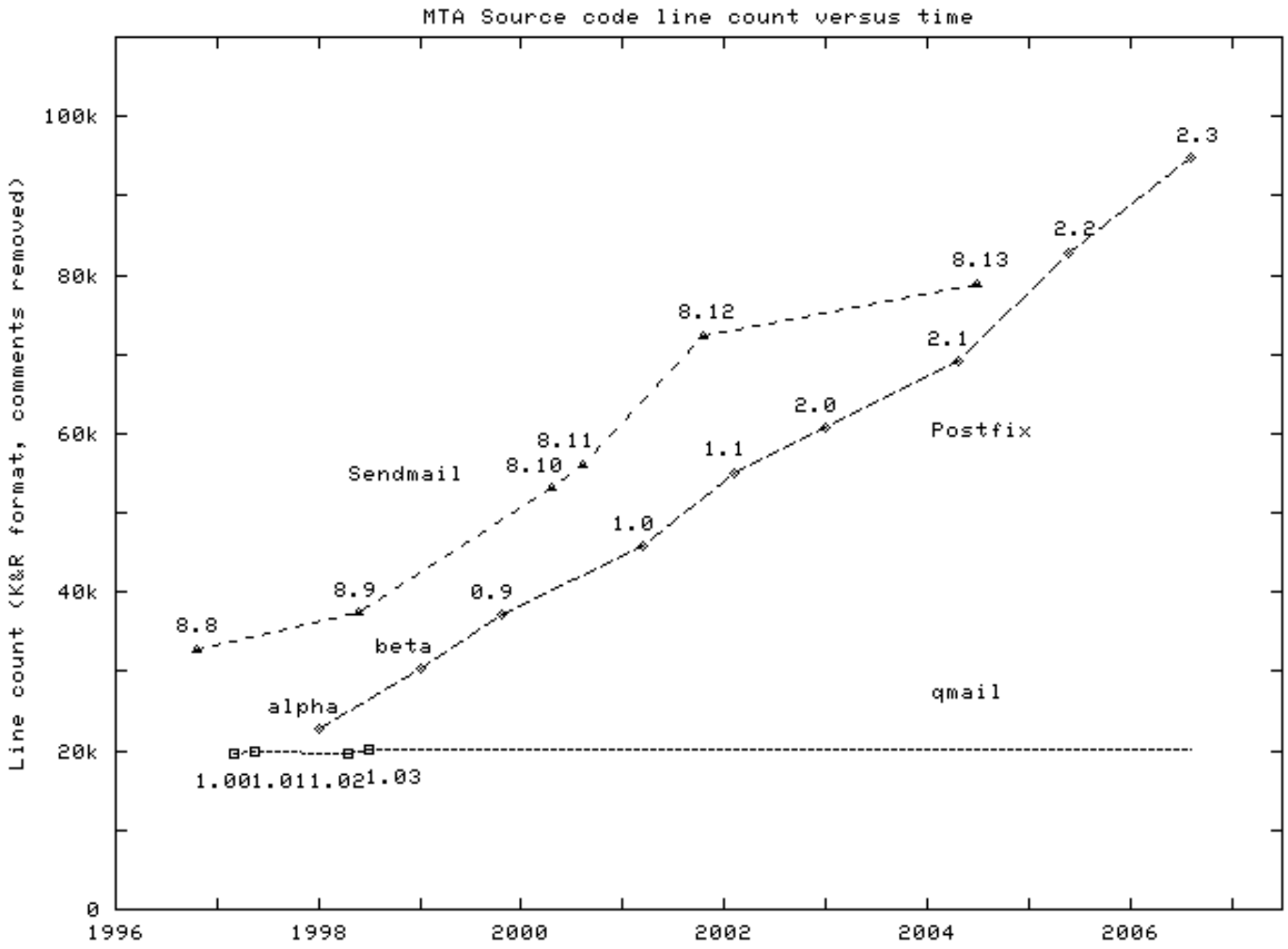
Die TLS-Handshakes sind sehr CPU-intensiv.
Das neue Limit
`smtpd_client_new_tls_session_rate_limit`
(standardmäßig deaktiviert) begrenzt die Anzahl von neuen (d.h. ungecachten) TLS Sitzungen.

- Daemonen die keine root-Rechte brauchen können nun nicht mehr als “privileged” gestartet werden
- sie **müssen** in der `master.cf` als “unprivileged” eingetragen sein
- konsequente Forcierung von “least privilege”

Beibehaltung der Groß-/Kleinschreibung bei Rewriting

- Postfix behält die Groß-/Kleinschreibung bei, wenn Adressen mittels `canonical`, `virtual`, `relocated` und `generic` Maps umgeschrieben werden
- sogar wenn `$zahl`-Ersetzungen durch reguläre Ausdrücke vorgenommen werden (`pcre` und `regexp`)
- `local(8)` und `virtual(8)` wandeln in Kleinschreibung um!

Code vs. Time


MTA Source code line count versus time
Line count (K&R format, comments removed)
100k
80k
60k
40k
20k
0
1996
1998
2000
2002
2004
2006
Sendmail
Postfix
qmail
8.8
8.9
8.10
8.11
8.12
8.13
beta
alpha
0.9
1.0
1.1
2.0
2.1
2.2
2.3
1.001.011.021.03

Postfix 2.4

Postfix 2.4 (28.03.2007)

poll/epoll

Unterstützung von:

- BSD `kqueue`
- Linux `epoll`
- Solaris `/dev/poll`

als Ersatz für `select()`

Verbesserung des worst-case Verhaltens des Queue-Manager beim Bouncing oder Deferring von vielen Mails. Der Queue-Manager redet nicht mehr synchron mit dem bounce oder defer daemon sondern asynchron über den neuen `retry` Daemon.

Milter Verbesserungen

Milters könnene jetzt auf den Inhalt einer Nachricht manipulieren.
Postfix implementiert nun alle Header/Body Manipulationen die Sendmail 8.13 erlaubt.

TLS

Dies und das. . .

Anpassung an greylisting

`queue_run_delay` und `minimal_backoff_time` wurden von 1000 auf 300 Sekunden reduziert, sodaß weitere Zustellversuche nach dem ersten Fehler schneller unternommen werden.

Resourcenschonung

`ipc_idle` wurde von 100 auf 5 Sekunden reduziert, sodaß `tlsmgr` und `scache` unbenutzte Dateideskriptoren schneller wieder freigeben.

Die Queue kann nun nach Site

- `postqueue -s site` und
- `sendmail -qRsite`

und sogar nach Queue-ID

- `postqueue -i queueid` und
- `sendmail -qIqueueid`

geflusht werden.

Bessere Interoperabilität mit kaputten Servern

Bessere Interoperabilität mit nicht standardkonformen SMTP Servern, die eine Nachricht vor dem Abschluß der `DATA` Phase mit einer Meldung abweisen und dann die Verbindung trennen.

Die individuellen Workarounds für die zahlreichen Fehler im `smtp protocl fixup` der CISCO PIX sind nun einzeln (de)aktivierbar:

- `smtp_pix_workarounds` (Standard: `disable_esmtp`, `delay_dotcrlf`)
- `smtp_pix_workaround_maps` (Workarounds nach IP Adresse (de)aktivieren)

Die Standardeinstellungen sind abwärtskompatibel.