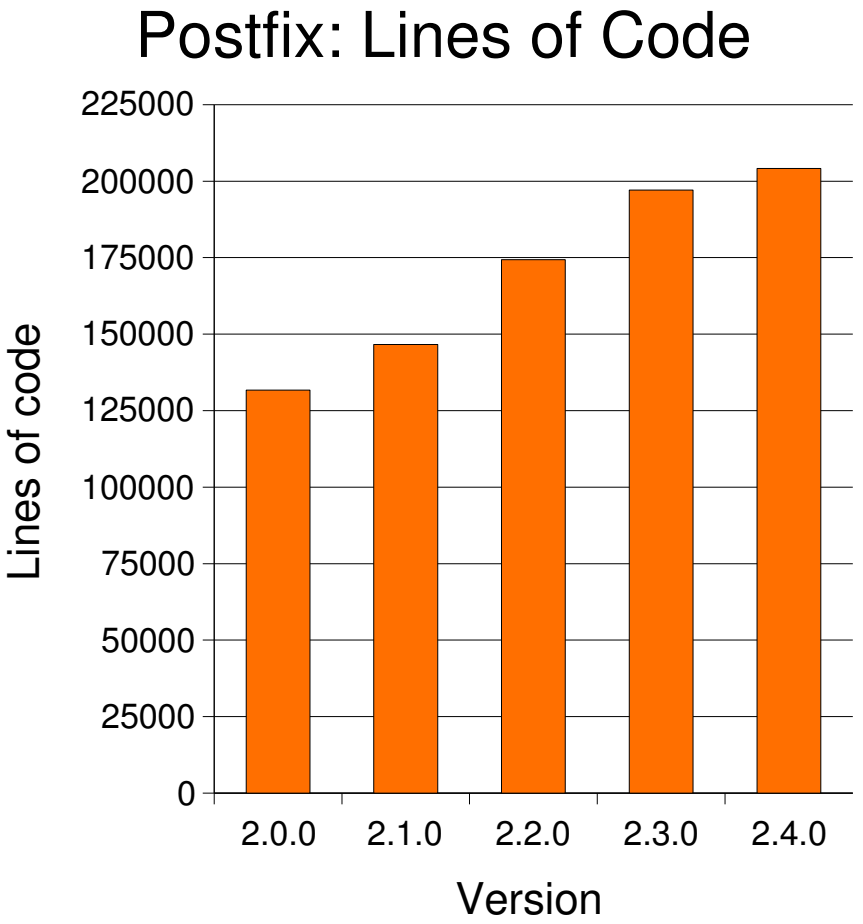
HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Postfix 2.0 bis 2.4: Was ist passiert?

- Postfix wurde in den letzten Jahren fast täglich weiterentwickelt
- Gerade für den Spam- und Virenschutz kamen viele schöne Funktionen dazu
- Trotzdem: Langsam kann Postfix alles, was man haben will...



HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Postfix 2.2, 2.3, 2.4 und die Zukunft: Was kommt nun?

- Wietse Venema über den status quo von Postfix:
  - **In 2006, Postfix 2.3 was mostly complete**. This was the result of a heroic effort to add enhanced status codes, DSN, and to make Postfix extensible with other SASL implementations, and last but not least extensible with Milters.
  - In 2007, Postfix 2.4 added a few missing pieces to Milter support, and a few performance improvements that help high-volume sites.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Tausend tolle Sachen...
Die vielen kleinen Änderungen

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SMTP und LMTP: Es wächst zusammen, was zusammen gehört

- LMTP wurde in das Modul „smtp“ integriert
  - Das Modul ist in /usr/lib/postfix doppelt vorhanden.
- Fast alle smtp_*-Parameter gibt es nun auch als lmtp_*-Parameter
  - Viele neue Features für LMTP gratis dazu :-):
    SSL/TLS für LMTP
    Shared Connection Caching für LMTP
- fallback_relay wurde zur Klarheit in smtp_fallback_relay umbenannt
  - Der alte Namen geht natürlich weiterhin.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Sender Dependend Relayhosts

- Bislang gab es nur relayhost= und fallback_relay=

  (bzw. smtp_relayhost= und smtp_fallback_relay=)

  - Problem 1: Manche Mailserver/Freemailer erlauben nicht die Einlieferung fremder Absenderdomains.
  - Problem 2: Findet man SPF toll, ist Outbound-Routing nötig.
  - [Man merke: SPF ist nicht toll. Aber das ist ein anderes Thema.]
- Nun ein neues Kommando für die main.cf:
  - sender_dependent_relayhost_maps = hash:/etc/postfix/sender_relay
- Die relayhost_maps ist eine klassische Lookup-Table:
  - Erste Spalte: Absender Zweite Spalte: Relayhost

```
user@firma.de                   mx-out1.firma.de
user@freemaildomain.local       smtp.freeaildomain.local
```

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Sender Dependent SASL-Authentication

- Sender Dependent Relayhosts erfordern ggf. auch unterschiedliche SASL-Logindaten für jeden Nutzer
  - smtp_sender_dependent_authentication=yes aktiviert das Feature
- Postfix fragt die smtp_sasl_password_maps dann zuerst nach der Sender-Mailadresse ab, dann wie bisher nach Zielhost/Domain.
- Sender Dependend Authentication deaktiviert Connection Caching für diesen Zielhost
- Macht nix, große Freemailer haben unterschiedliche Hosts für User-SMTP- und MX-Inbound

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Pimp my Mailversand (1)

- Verbindungsauf- und abbau kostet Kraft & Zeit:
  - TCP/IP-Handhshake
  - DNS-Lookups
  - HELO-Kommando
  - (Wechsel zu SSL/TLS)
- Connection-Caching nutzt vorhandene Verbindungen
  - max_conn_use=
- Neues Logfileformat:

```
Jun 16 18:48:40 ilpostino postfix/smtp[12532]: 6CC688C222: to=<mimibreig@web.de>, relay=mx-
ha01.web.de[217.72.192.149]:25, conn_use=2, delay=21, delays=0.85/19/0.02/0.6, dsn=2.0.0,
status=sent (250 OK id=1HzbS3-0001sV-00)
Jun 16 18:48:40 ilpostino postfix/smtp[12532]: 6CC688C222: to=<mimicho@web.de>, relay=mx-
ha01.web.de[217.72.192.149]:25, conn_use=3, delay=21, delays=0.85/20/0.02/0.65, dsn=2.0.0,
status=sent (250 OK id=1HzbS4-0001sV-00)
```

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Pimp my Mailversand (2)

- Alle smtp-Client-Prozesse benutzen ein gemeinsames (shared) Connection-Caching:
  - Nach Verbindungsende übergibt smtp die Verbindung an scache.
  - Sinnvoll: Der smtp gibt Verbindungen zu scache nur für Server, die noch viele Mails in der Queue haben: smtp_connection_cache_on_demand = yes
  - Alternativ: smtp_connection_cache_destinations listet manuell zu cachende Verbindungen. Syntax wie $mydestination: Direkte Liste oder lookup-Table
  - scache hält die Verbindung maximal smtp_connection_cache_time_limit = 2s!
  - (Sendmail und Exim können kein shared caching...)
- Das neue scache-Modul ist in der master.cf definiert:
  - scache unix - - n - 1 scache

Pimp my Mailversand (3)

- (Shared) Connection Caching geht nicht bei SSL/TLS-Verbindungen
- Alle connection_cache_status_update_time loggt scache seine Statistik:

```
Jun 16 13:56:08 ilpostino postfix/scache[4610]: statistics: start interval Jun 16 13:47:36
Jun 16 13:56:08 ilpostino postfix/scache[4610]: statistics: domain lookup hits=6 miss=29
success=17%
Jun 16 13:56:08 ilpostino postfix/scache[4610]: statistics: address lookup hits=0 miss=155
success=0%
Jun 16 13:56:08 ilpostino postfix/scache[4610]: statistics: max simultaneous domains=13
addresses=13 connection=13
```

  - Domain lookup: Caching anhand Recipient-Domain
  - Address Lookup: Caching über die IP des MX-Servers

Analyse my Mailversand

- Postfix loggt einen neuen „delay“-Wert: delays=a/b/c/d

```
Jun 16 18:48:40 ilpostino postfix/smtp[12532]: 6CC688C222: to=<mimibreig@web.de>,
relay=mx-ha01.web.de[217.72.192.149]:25, conn_use=2, delay=21, delays=0.85/19/0.02/0.6,
dsn=2.0.0, status=sent (250 OK id=1HzbS3-0001sV-00)
```

- So kann genauer der Flaschenhals analysiert werden:
  - a=Zeit bis die Mail in der Queue war (d.h. inkl. Empfangszeit)
  - b=Zeit, die die Mail in der Queue war
  - c=Zeit für den Verbindungsaufbau (DNS, HELO und TLS)
  - d=Übertragungszeit für den Versand
  - a+b+c+d = delay
- Alle Angaben in Sekunden

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Was nicht passend ist, wird passend gemacht

- Endlich wurden ein paar verwirrende Optionen der Restrictions umbenannt:
  - reject_unknown_client => reject_unknown_client_hostname
  - reject_unknown_hostname => reject_unknown_helo_hostname
  - reject_invalid_hostname => reject_invalid_helo_hostname
  - reject_non_fqdn_hostname => reject_non_fqdn_helo_hostname
- Danke!
- Die alten Namen funktionieren weiterhin.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Die neue Milter-Schnittstelle: Sendmail muß nicht immer schlecht sein...

- Milter ist die Schnittstelle für Filter-Plugins unter Sendmail
- milter ist ein pre-queue-Filter
- Postfix hat diese Implementiert => Milter-Pakete sind nun nutzbar

- Vorsicht: Postfix 2.3 ändert darum seine Queue-Struktur!
- Update ist kein Problem
- Wenn Wechsel von >= 2.3 zurück (!) zu <= 2.2 droht Mailverlust jedoch nur, wenn Milter auch tatsächlich aktiv benutzt wurde

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Individuelle Bounce-Templates

- Früher: Neukompilieren!
- Jetzt im Stile von HERE-Dokumenten gelöst:
  - bounce_template_file verweist aus main.cf auf Vorlage
  - /etc/postfix/bounce.cf.default dient als Beispiel
- Englische Fassung nicht vergessen!
- Deutsche Templates:
  - http://postfix.state-of-mind.de/bounce-templates/

```
failure_template = <<EOF
Charset: us-ascii
From: MAILER-DAEMON (Mail Delivery System)
Subject: Undelivered Mail Returned to Sender
Postmaster-Subject: Postmaster Copy: Undelivered Mail

This is the $mail_name program at host $myhostname.

I'm sorry to have to inform you that your message
could not be delivered to one or more recipients.
It's attached below.

For further assistance, please send mail to
<postmaster>

If you do so, please include this problem report. You
can delete your own text from the attached returned
message.

                   The $mail_name program
EOF
```

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Und viele andere Kleinigkeiten

- Rate-Limiting für SSL_/TLS-Clients möglich
  - smtpd_client_new_tls_session_rate_limit
- Authentifzierungsbibliotheken per Plugin unterstützt
  - Neben Cyrus-SASL jetzt auch Dovecot-SASL & CO
- Postfix behält Groß-/Kleinschreibungen in den verschiedenen Lookup-Tables bei
  - canonical, virtual, relocated und generische Lookup-Tables achten drauf
  - Weiterleitungen an Klaus_Mueller@Firma-GmbH.local sind möglich
- Keine rekursiven Ersetzungen mehr per pcre-/regexp-Tables!
- Grundlegende Überarbeitung/Erweiterung von SSL/TLS
  - Neue Sicherheitsstufen möglich; SSL/TLS ohne feste Zertifikate möglich

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Enhanced Status Codes und Delivery Status Notications im Detail

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Enhanced Status Codes (ESN)

- Normale Fehlermeldungen können zu wenig Informationen über den Grund des Fehlers geben.
- Insb. automatische Auswertung der Bounces sind unmöglich
- DSN liefert ein großes Set definierter möglicher Fehler
- Auch Benachrichtigungen über erfolgreiche Zustellungen sind möglich.

```
X.2.0 Other or undefined mailbox status
X.2.1 Mailbox disabled, not accepting messages
X.2.2 Mailbox full
X.2.3 Message length exceeds administrative limit.

X.5.0 Other or undefined protocol status
X.5.1 Invalid commanda
X.5.2 Syntax error
X.5.3 Too many recipients
X.5.4 Invalid command arguments
X.5.5 Wrong protocol version

X.7.0 Other or undefined security status
X.7.1 Delivery not authorized, message refused
X.7.2 Mailing list expansion prohibited
X.7.3 Security conversion required but not possible
X.7.4 Security features not supported
X.7.5 Cryptographic failure
X.7.6 Cryptographic algorithm not supported
X.7.7 Message integrity failurec
```

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Enhanced Status Codes (ESN): Warum-wieso-weshalb?

- SMTP-Codes waren nicht eindeutig genug; genaue Codes sind aber für Delivery Status Notifications (DSN) erwünscht
  - Aus alt...: 550 User unknown
    Mach neu: 550 5.7.0 User unknown
- Diese können, müssen aber nicht ausgewertet werden; der SMTP-Code klärt bereits die Fakten auf Zustellebene:
  - 2xx: Status Okay
  - 4xx temporärer Fehler
  - 5xx fataler / dauerhafter Fehler
- ESN sind derzeit eher auf inhaltlicher Ebene interessant, d.h. warum/wo/wie etwas nicht zugestellt wurde etc.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Enhanced Status Codes (ESN): Hier sind sie definiert!

- Der Status-Code hat drei Teile: classe . subject . detail
  - 2.x.x = Erfolg
  - 4.x.x = temporärer Fehler
  - 5.x.x = fataler Fehler
- Enhanced Status Codes stammen aus RFC 3463: http://www.faqs.org/rfcs/rfc3463.html

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Enhanced Status Codes (ESN): So werden Sie benutzt.

- Die Codes können in access_maps, header/body_checks etc. benutzt werden:
  - user@domain.local REJECT 5.7.1 You're not authorized to send this e-mail
- soft_bounce=yes paßt auch die Enhanced Status Codes an
  - Aus 5.x.x wird 4.x.x
- Postfix korrigiert auch sender/recipient-codes:
  - Wird eine access_map für sender- und recipient-lookups gleichzeitig genutzt, wird aus einem
    5.1.4 (Bad destination mailbox address syntax) ggf. ein
    5.1.7 (Bad sender's mailbox address syntax)

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Delivery Status Notifications (DSN): Warum-wieso-weshalb?

- DSN machen die ESN für uns nutzbar
- Insgesamt vier Kategorien: success, failure, delay oder none
  - Default: delay, failure (also wie immer!)
- Absender kann angeben, über was er informiert werden will
  - Über eine Erweiterung des ESMTP-Befehlssatzes
  - Über neue Parameter für /usr/bin/sendmail:
    sendmail -N success,delay,failure [...]
- DSN können auch vorgeben, welche Teile der Mail bei einem Bounce zurückgeschickt werden sollen
  - header oder body`

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Delivery Status Notifications (DSN): Die Envelope-ID taggt Mails

- DSN implementiert auch eine Envelope-ID, die von Server zu Server weitergereicht und beim Bouncen zurückgeschickt wird
- So können unzustellbare Nachrichten beim Massenversand identifiziert werden
- Ersetzt alte VERP-Mechanismen – nicht verwechseln
  - Angabe wieder über erweiterten ESMTP-Befehlssatz
  - Oder über neuen Parameter:
    sendmail -V <envelope-id> [...]
  - Die Envelope-ID ist nicht identisch mit der Message-ID!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Delivery Status Notifications (DSN): Die ESMTP-Erweiterungen

- MAIL FROM und RCPT TO wurden optional erweitert:
  - MAIL FROM: <user@domain.de> RET=[FULL|HDRS]
    Bei einem Bounce wird [alles|nur der Header] zurückgeschickt
  - MAIL FROM: <user@domain.de> ENVID=“text-id“
    Legt die Envelope-ID fest, die beim Bounce zur Identifizierung zurückgeschickt werden soll.
  - RCPT TO: <user@domain.de> NOTIFY=[NEVER|SUCCESS,FAILURE,DELAY]
    Der Absender fordert DSN für (k)eine dieser Kategorien an
  - RCPT TO: <user@domain.de> ORCPT=rfc2822;user@olddomain.de
    Gibt den ursprünglichen Empfänger an, von dem aus weitergeleitet wurde („virtual“-maps).

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Delivery Status Notifications (DSN): So outet sich der Server

- Die Fähigkeit zu DSN wird per ESMTP bekannt gegeben:

```
220 peer.post.fix ESMTP Postfix
EHLO mail.domain.local
250-peer.post.fix
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

- Unter Umständen nerven DSNs jedoch oder sind unerwünschte Serverbelastung.
- Erfolgreiche Zustellbestätigungen ein Sicherheitsproblem sein!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Delivery Status Notifications (DSN): Selektiv an-/abschalten

- Einzelne DSN-Features kann man nicht ausblenden.
  - Also: Ganz oder gar nicht!
  - DSN sind nur möglich, wenn sich der Server nach EHLO outet!
- Global in /etc/postfix/main.cf:
  - smtpd_discard_ehlo_keywords = silent-discard, dsn
- Oder selektiv je nach Client:
  - smtpd_discard_ehlo_keyword_address_maps = cidr:/etc/postfix/esmtp_access legt fest, für welche Netze kein DSN announct wird:

```
/etc/postfix/esmtp_access:
# DSN für 192.168.0.0/16 erlauben
192.168.0.0/16      silent-discard
0.0.0.0/0           silent-discard, dsn
::/0                silent-discard, dsn
```

  - Das Keywort „silent-discard“ verhindert entsprechende Logmeldungen

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Delivery Status Notifications (DSN): Das passiert, wenn sie geblockt werden

- Am ersten Nicht-DSN-Host endet die Verfolgung.
- Nimmt man kein DSN am MX-Gateway an, wird der einliefernde Mailserver jedoch noch das erfolgreiche weiter-relayen zurückmelden.
- Dagegen ist sicherheitstechnisch aber nichts einzuwenden.
- Für den Absender ist i.d.R. aber ausreichend zu wissen, daß die Zustellung an das MX-Relay erfolgreich war.
- Wann/wo/wie MX-Relay in das Zielpostfach geschrieben hat, muß Absender nicht wissen.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Ja...und nun?

- Update aufgrund verschiedener Performancezuwächse durchaus erstrebenswert.
- Gerade auch die ESN/DSN-Unterstützung sollte in unser aller Interesse sein.
- Postfix 2.4.x dürfte eine Basis sein, auf der man sich lange ausruhen kann. Ein Update jetzt macht auch für konservative Update-Politik Sinn.
- Aber grundsätzlich gilt natürlich: Wer keine Schmerzen hat, muß auch nicht krampfhaft neues ausprobieren.
- Grundsätzlich ist ein Update kein wirkliches Problem. Doch der Teufel steckt im Detail.
- Ihr wißt ja: Never change a running system

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Für die, die nicht genug kriegen können

- Das Postfix-Buch von mir bei Open Source Press
  http://www.postfixbuch.de
- Übrigens: Komplett überarbeitete 3. Auflage im späten Herbst.
- Hat dann alles, was man braucht und wissen muß:
  - Die ganzen neuen Features und Änderungen
  - Mehr LDAP
  - Richtig schön amavisd-new / SpamAssassin
  - Noch mehr Tipps und Best Practice mit vielen Empfehlungen aus der Praxis
- Die Postfixbuch-Mailingliste:
  http://listi.jpberlin.de/mailman/listinfo/postfixbuch-users

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Für die, die konkrete Hilfe brauchen

- Wir sind die Mailserver-Schmiede:
  - Troubleshooting im Notfall
  - Consulting & Installation, auch Cluster-Installationen mit > 250.000 Nutzern
  - HA Anti-Spam/Viren-Relays
  - Groupware-Lösungen und Migrationsstrategien
- 24/7 CompetenceCall mit LPIC-2-Admins: 030/40 505 - 110
- Postfix-Kurse an unserer Akademie oder inhouse bei Ihnen
- Mail-Outsourcing in unser Rechenzentrum

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Was ich noch zu sagen hätte...

- Bei Fragen: Fragen!

- Und ansonsten: Danke für Eure Aufmerksamkeit und noch eine schöne weitere Konferenz!