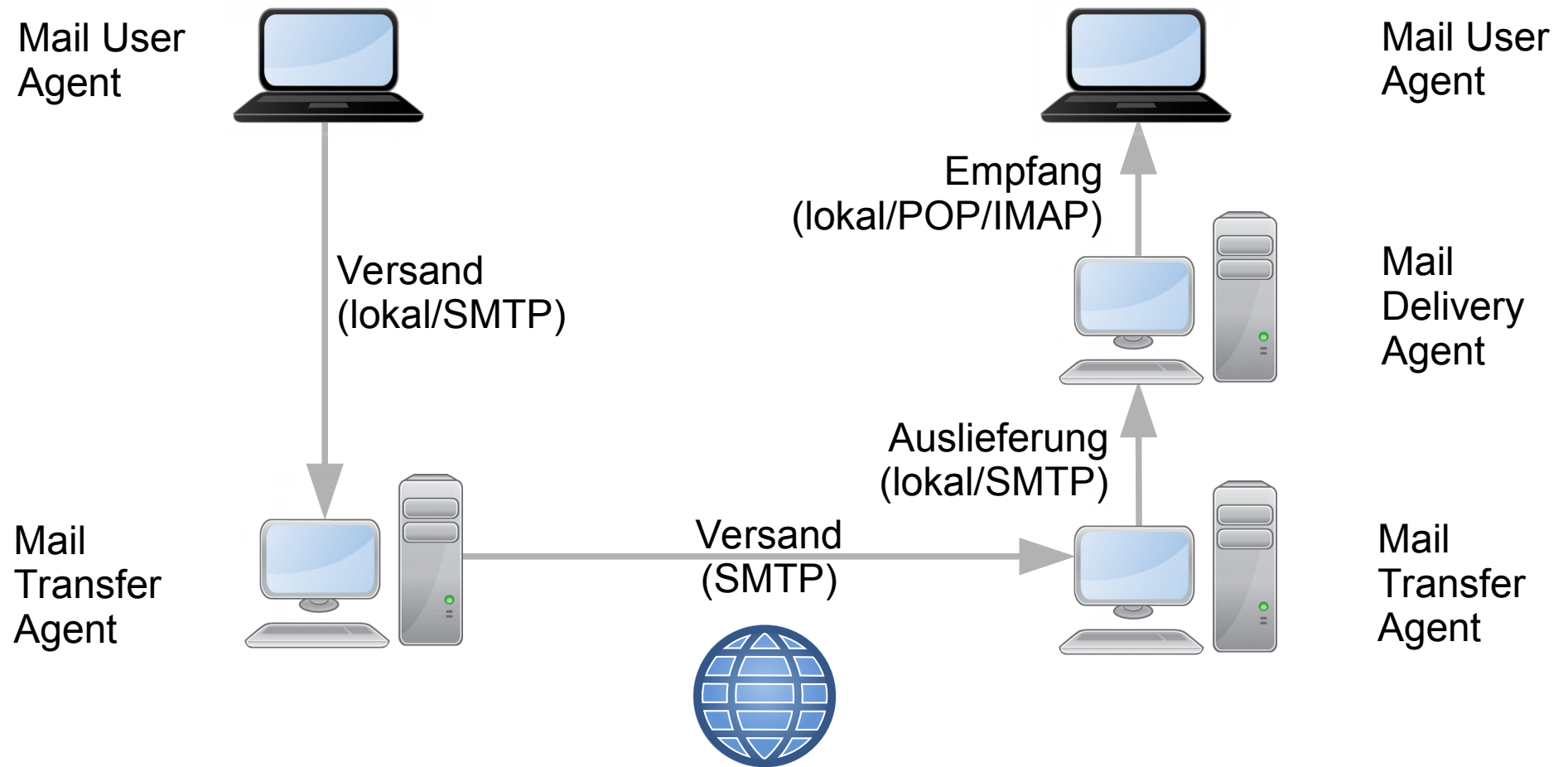


Betrieb eines E-Mail Servers unter Linux

Linux-Workshop Köln
7. Mai 2019

Harald Weidner
hweidner@gmx.net

Funktionsweise E-Mail



E-Mail Komponenten

Mail Transfer Agent (MTA)

- Empfang und Versand von E-Mail per SMTP
- z.B. Postfix, Sendmail, Exim, Qmail

Mail User Agent (MUA)

- Lesen und Schreiben von E-Mails
- Versand mit SMTP, Empfang mit POP/IMAP
- Thunderbird, mutt, Claws Mail, Evolution

Mail Delivery Agent (MDA)

- Verarbeitung und Auslieferung empfangener Mails
- z.B. procmail, maildrop, Sieve

Weitere E-Mail Komponenten

Webmailer

- Gateway zwischen Browser und MTA/MDA
- z.B. Roundcube, SquirrelMail, Horde/IMP, Mailpile

POP/IMAP Server

- z.B. Dovecot, Courier, Cyrus

Spamfilter, Virenschutz etc.

- z.B. milter, amavis, Spamassassin, Postgrey

Weitere Tools und Infrastruktur

- z.B. formail, mail-expire, fetchmail, getmail, biff, uucp
- DNS Blacklists

E-Mail Server Anforderungen

Zwingend erforderlich

- Statische IP-Adresse
- MX Record
- A- und PTR Records
- Relaying-Schutz

Nice to Have

- SPF / DKIM
- DNSSEC / DANE
- Spamfilter
- Virenschutz

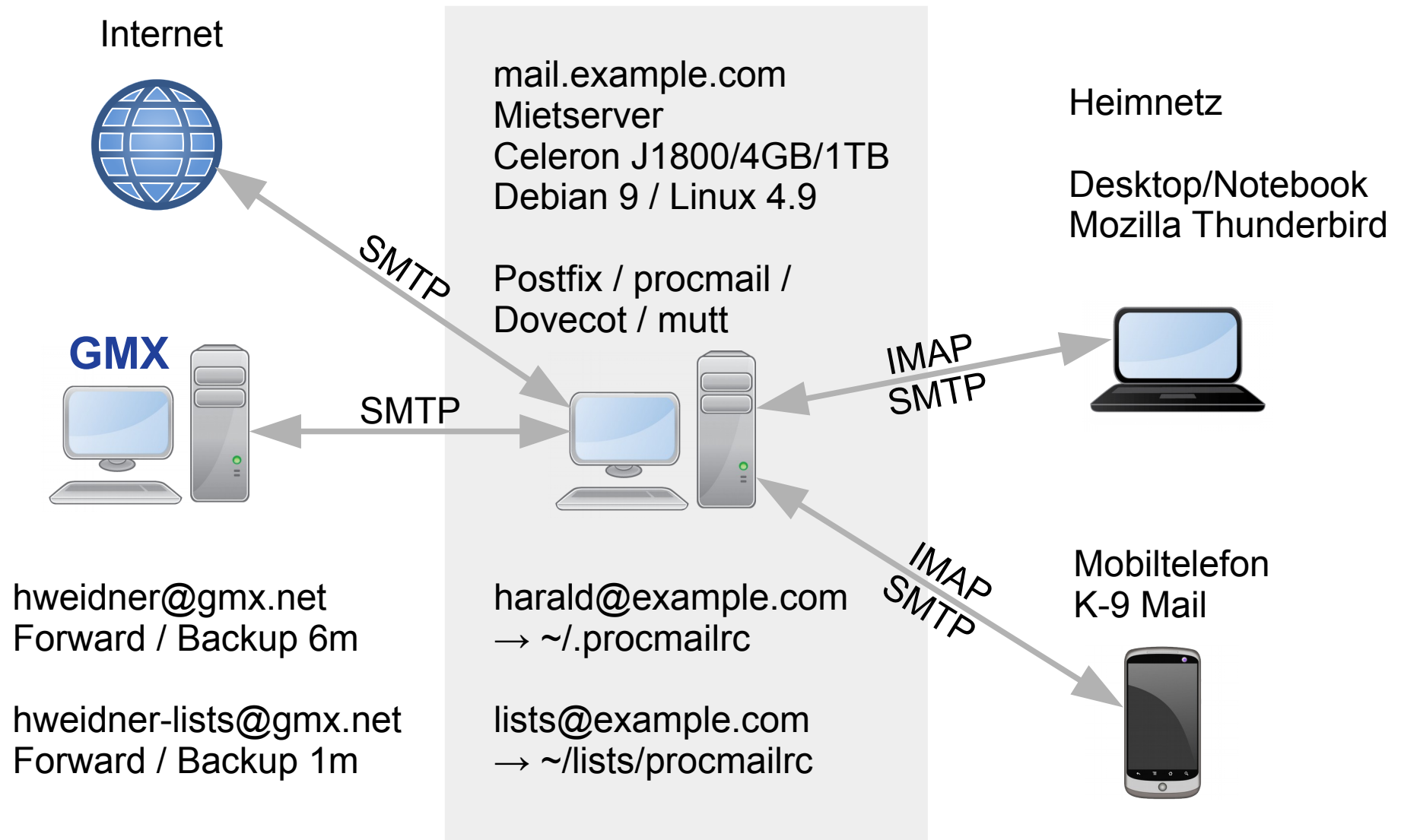
Empfehlenswert

- STARTTLS Client
- STARTTLS Server

(Noch?) nicht verbreitet

- RMX / DMARC
- DNScurve

Mein E-Mail Setup



DNS Konfiguration

- Einträge für MX, A/AAAA und PTR

Zone example.com

```
@      IN  MX      10 mail.example.com
mail   IN  A       10.20.30.40
mail   IN  AAAA    2001:db8:85a3::8a2e:370:7334
```

Reverse Records

```
40.30.20.10.in-addr.arpa.  IN  PTR  mail.example.com.
4.3.3.7.0.7.3.0.e.2.a.8.0.0.0.0.0.0.0.0.0.0.3.a.5.8.8.b.d.0.1.0.0.2.ip6.arpa.
                                IN  PTR  mail.example.com.
```

Postfix – Mail-Empfang

- Schutz vor Relaying und fehlerkonfigurierten Systemen

```
mydestination = example.com, mail.example.com [...]
mynetworks = 127.0.0.0/8 [::1]/128 [...]

smtpd_recipient_restrictions =
    permit_mynetworks,
    reject_unauth_destination,
    reject_invalid_hostname,
    reject_non_fqdn_hostname,
    reject_non_fqdn_sender,
    reject_non_fqdn_recipient,
    reject_unknown_sender_domain,
    reject_unknown_recipient_domain,
    [...]
    reject_rbl_client ix.dnsbl.manitu.net,
    reject_rbl_client bl.spamcop.net,
    permit
```


Postfix – Black- und Whitelist

- Matcht auf (Envelope-) Absendeadressen
- Eigene Domains dürfen nicht von außen kommen

Datei main.cf

```
smtpd_recipient_restrictions =  
    [...]  
    check_sender_access hash:/etc/postfix/sender_access,  
    [...]
```

Datei sender_access

```
# Whitelist  
nicedomain.com    OK  
  
# Blacklist  
example.com       REJECT  
.example.com      REJECT
```

Postfix – Netzwerkrestriktionen

- Matcht auf IP-Adressen / Domainnamen

Datei main.cf

```
smtpd_recipient_restrictions =  
    [...]  
    check_client_access hash:/etc/postfix/client_access,  
    [...]
```

Datei client_access

```
gmx.net          OK  
.gmx.net         OK  
  
unwanteddomain.com REJECT
```

Postfix – Weitere Maps

- `recipient_access`
 - Matcht auf (Envelope-)Empfänger-Adressen
- `helo_access`
 - Matcht auf HELO Hostnamen
- `transport`
 - Regeln für die Weiterleitung von E-Mails
- Die meisten Maps wahlweise als Hashtabelle oder RegExp-Liste (PCRE)
- Hash-Maps müssen mit `postmap` erzeugt werden

Postfix – Versand über GMX

- Versand über Provider-Accounts je nach Absender
- Default: direkte Zustellung über MX

Datei main.cf

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

Datei sender_relay

```
hweidner@gmx.net      [mail.gmx.net]
hweidner-lists@gmx.net [mail.gmx.net]
```

Datei sasl_passwd

```
hweidner@gmx.net      hweidner@gmx.net:password1
hweidner-lists@gmx.net hweidner-lists@gmx.net:password2
```

Sortierung mit Procmail

Datei /etc/postfix/main.cf

```
mailbox_command = procmail -a "$EXTENSION"
```

Datei ~/.procmailrc

```
MAILDIR=$HOME/Mail
```

```
LOGFILE=$HOME/.procmail/log_`date +%Y-%m`
```

```
EXT=$1
```

```
# Filter nach Absender
```

```
:0:
```

```
* ^From:.*test@testdomain\.com
```

```
test
```

```
# Filter nach Extension (an harald+example@example.com)
```

```
:0:
```

```
* ? [ "$EXT" = "example" ]
```

```
example
```

Generische Sortierung

- Erkennt Mails von Mailinglisten und sortiert die in passende Mailboxen

```
# Detect mailing lists
:0
* !^X-Mailing-List:[ ]<\#[^ >`']+
* !^X-Mailing-List:[ ]\#[^ `']+
* !^Sender:[ ]owner-\#[^ `']+
* !^X-BeenThere:[ ]\#[^ `']+
* !^Delivered-To:[ ]mailing list \#[^ `']+
* !^X-Loop:[ ]\#[^ `']+
* !^List-Post:[ ]<mailto:[^ >`']+>
{ }
:0 E
{
:0:
$MAIL/`echo $MATCH | sed -e 's/[\/]/_/g' | tr A-Z a-z`
}
```

Anzeigen von Mailinglisten

Datei ~/.bashrc

```
alias lists='mutt -y -F $HOME/lists/muttrc'
```

Datei ~/lists/muttrc

```
mailboxes `find ~/lists/Mail/ -name ".*" -type f -printf '%p '`
```

```
set sort = threads
```

```
set sort_aux = reverse-last-date
```

```
set folder_format = "%3C %t %N %8s %d %f"
```

```
my_hdr From: Harald Weidner <hweidner-lists@gmx.net>
```

```
set sendmail = "/usr/sbin/sendmail -oi \  
-f hweidner-lists@gmx.net"
```

Alternativen zum eigenen Server

E-Mail Provider

- z.B. GMX, WEB.DE, GMAIL, Posteo, Mailbox.org
- i.d.R. mit Web-Mail, SMTP-Versand, POP/IMAP
- Teilweise eigene Domains möglich

E-Mail-Funktion des Access Providers

- z.B. t-online, 1&1, Unitymedia, ...
- Problematisch bei Providerwechsel

Provider mit Shell-Account

- z.B. hostsharing.net (Debian), uberspace.de (CentOS)
- Sehr viele Konfigurationsmöglichkeiten