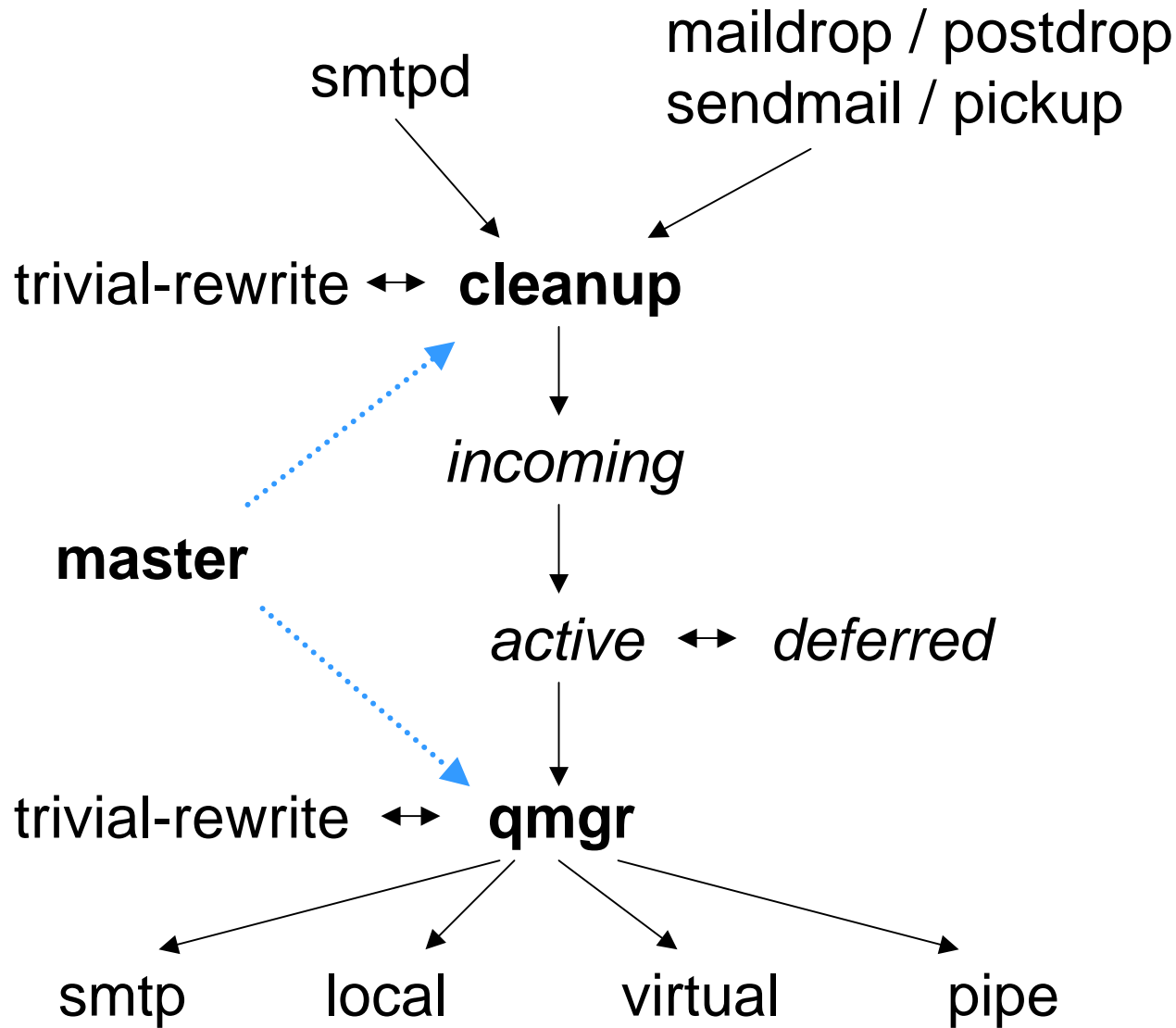


Postfix Mini-Einführung

Sebastian Werner

- Entwickelt im Hause IBM von Wietse Venema (seit 1998)
 - Steht unter der IBM Public License, heisst offiziell: *IBM Secure Mailer / Postfix*
- Modularer Aufbau
- Einfache, übersichtliche Konfiguration
- Gute Dokumentation
- Regelmäßige Updates (vgl. Qmail)
- Vielfalt an Features



Einlieferung

Auslieferung

- Werden verwendet für Lookups aller Art (z.B. Usertabellen, ACL, Blocks, Transports)
- Simple *Key* → *Value* Verzeichnisse
- Typen
 - btree, hash, cdb
 - ldap, unix, nis
 - Mysql, pgsql
- Zusätzlich: Regular Expression Maps

Mapping von Usern

- Lokaler User: Hauptdomain des Servers wird auf Benutzer (uid) mapped
/etc/aliases, (unix|nis):passwd.byname,
- Virtuelle Nutzer: Über eine Datenbank werden user@host auf ein lokales Verzeichnis übertragen.
Datenbank, virtual-map, LDAP, ...
- Weitergehendes Rewriting für alle Fälle:
http://www.postfix.org/ADDRESS_REWRITING_README.html

- Legen fest, welchen Weg eine bestimmte Mail nimmt
- Möglichkeit, externe Programme einzubinden
 - Mailman
 - Spamd
 - Amavis
 - ...

- Speziell bei smtpd kann pro „Status“ der Session gefiltert werden
smtpd_*STATUS*_restrictions
- Konkret:
 - client: Zu Beginn einer SMTP Session
 - helo: HELO command
 - sender:MAIL FROM: (Envelope)
 - recipient: Zu RCPT TO: (Envelope=
 - data: Die eigentliche Mail.
- Praktisch: Alle ACL in einer: recipient!

Typisches Anforderungsprofil

- Virtuelles Domainhosting
- Mailinglisten
- Relay-Service für Nutzer
- Spam-Minimierung
- Serverseitiges Filtern/Sortieren von Mails
- Zugriff via IMAP oder lokal

- Mailinglisten via Mailman
- Relay: TLS, smtp-auth mit SASL
- Anti-Spam: Policyd-weight, Postgrey & spamd
- Serverseitiges sortieren: procmail oder sieving

Basic settings

```
myorigin = /etc/mailname
myhostname = erlangen.ccc.de
mydomainname = erlangen.ccc.de
# local destinations
mydestination = erlangen.ccc.de,
    localhost.net, localhost
# trusted networks
mynetworks = 127.0.0.0/8
# gateway für mailman
relay_domains = lists.erlangen.ccc.de
```

incoming: smtpd

```
smtpd_use_tls=yes
smtpd_tls_cert_file=/etc/ssl/certs/x.crt
smtpd_tls_key_file=/etc/ssl/private/x.key
smtpd_tls_session_cache_database =
    btree:${queue_directory}/smtpd_scache
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 24h
smtpd_banner = $myhostname ESMTP $mail_name
smtpd_recipient_limit = 50
smtpd_soft_error_limit = 3
smtpd_hard_error_limit = 12
```

incoming: smtpd - smtpauth

```
smtpd_sasl_auth_enable = yes
smtpd_tls_auth_only = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_application_name = smtpd
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
broken_sasl_auth_clients = yes
smtpd_sasl_authenticated_header = yes
```

outgoing: smtp

```
smtp_tls_security_level = may
smtp_tls_session_cache_database =
    btree:${queue_directory}/smtp_scache
smtp_tls_session_cache_timeout = 24h
smtp_helo_timeout = 300s
```

```
smtpd_restriction_classes = greylisting
greylisting = check_policy_service
    inet:127.0.0.1:60000
```

```
smtpd_helo_required = yes
smtpd_data_restrictions =
    reject_multi_recipient_bounce,
    reject_unauth_pipelining
smtpd_recipient_restrictions = <next slide>
```

Die Anti-Spam ACL

```
smtpd_recipient_restrictions=  
permit_mynetworks  
permit_sasl_authenticated  
reject_invalid_helo_hostname  
reject_non_fqdn_sender  
reject_non_fqdn_recipient  
reject_unknown_recipient_domain  
reject_unlisted_recipient  
reject_unauth_destination  
check_client_access pcre:/etc/postfix/postgrey.map  
reject_unknown_sender_domain,  
check_policy_service inet:127.0.0.1:12525,  
permit_auth_destination,reject
```

Lineare Abarbeitung bis *reject* oder
accept rauskommt (Default: *dunno*)



Lokale / Virtuelle User

```
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases

local_recipient_maps = $alias_maps
    unix:passwd.byname

home_mailbox = .maildir/
mailbox_command = /usr/bin/procmail -a
    "$EXTENSION,"

virtual_alias_domains = bitsnbugs.de
virtual_alias_maps =
    hash:/etc/postfix/virtual
```


Mailman einbinden

```
transport_maps = hash:/etc/postfix/transport
```

dort:

```
erlangen.ccc.de      :  
lists.erlangen.ccc.de mailman:
```

```
mailman_destination_recipient_limit = 1
```

```
owner_request_special = no
```

```
biff = no
append_dot_mydomain = no
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
maximal_queue_lifetime = 7d
minimal_backoff_time = 1000s
maximal_backoff_time = 8000s
```

Was im Hintergrund läuft

- Mailman als Listen-Manager
- Dovecot als Full-Featured IMAPd
- Dovecot-SASL als Authentifizierungs-Backend
- Policyd-weight zum Blocken von Spam-Hosts (Punktevergabe für Protokollverletzungen, Auftauchen in RBLs, Hammering, ...)
- Postgrey für Dial-Up Hosts
- Spamd zum Taggen von Spam

Tips zum Weiterlesen

- <http://www.postfix.org>
- <http://postfix.wiki.xs4all.nl>
- [www.gnu.org/software/**mailman**/](http://www.gnu.org/software/mailman/)
- <http://www.policyd-weight.org>
- <http://www.dovecot.org>

Thanks for your attention!

Questions or Suggestions?!