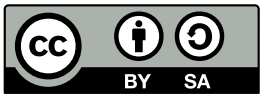
Mailserver Teil 2

Andreas Teuchert

23. Februar 2015



Mails von außen

- von wem werden E-Mails von außen angenommen?
  - `inet_interfaces`
  - `inet_protocols`
  - `mynetworks`
  - authentifizierte Clients
- für wen werden E-Mails angenommen?
  - `mydestination`
  - `relay_domains`
  - `virtual_alias_domains`, `virtual_mailbox_domains`
  - Mail-Versand für authentifizierte Clients

Von wem?

- `inet_interfaces` legt fest, auf welchen Netzwerk-Interfaces Postfix Verbindungen von außen annimmt
- `inet_interfaces = loopback-only`: keine Verbindungen von außen
- `inet_interfaces = all`: Verbindungen werden auf allen Interfaces angenommen
- oder explizit IP-Adressen der Netzwerk-Interfaces angeben
- `inet_protocols` legt die aktivierten Netzwerk-Protokolle (IPv4, IPv6) fest
- `inet_protocols = all`: beides aktivieren

Mit diesen Einstellungen lässt sich festlegen, wer sich auf Netzwerk-Ebene mit dem Mailserver verbinden kann. Dies bedeutet nicht, dass der Mailserver dann auch E-Mails von diesen Clients annimmt. Dazu müssen noch weitere Einstellungen festgelegt werden.

mynetworks

- legt die IP-Adressbereiche fest, für die der Server Mail-Relay ist
- von diesen IP-Adressen können E-Mails an beliebige Adressen über den Server versandt werden
- üblicherweise nur Localhost-Adressen
- falls der Server Mail-Relay ist, auch lokales Netzwerk
- niemals fremde Adressen eintragen!

Diese Einstellung ist wichtig, wenn der Server von lokalen Clients ohne weitere Authentifizierung als Mail-Relay verwendet werden soll. Diese Netzbereiche müssen dann in `mynetworks` aufgeführt sein. Da der Server für diese Adressbereiche E-Mails an beliebige Empfänger annimmt und versendet, dürfen hier niemals fremde Adressen eingetragen werden.

Clients außerhalb dieser Adressbereiche können sich per Authentifikation mit Benutzername und Passwort legitimieren und dann den Server als Relay verwenden.

mydestination

- Liste von Domains, für die lokale Mailboxen auf dem Server vorhanden sind
- Adressen (vor dem @) entsprechen lokalen Benutzern
- üblicherweise `localhost` und der Hostname des Servers eingetragen
- wenn der Server für die Domain des Mailservers zuständig ist, auch diese
- es können auch fremde Domains eingetragen werden (wenn ein entsprechender MX-Eintrag gesetzt ist)
- aber meistens nicht sinnvoll, da alle gleichen Adressen (vor dem @) unter verschiedenen Domains dem gleichen lokalen Benutzer zugeordnet werden

Auch wenn beliebig viele Domains als `mydestination` eingetragen werden können, ist dies eher unüblich. Dies führt nämlich dazu, dass nur Benutzer mit lokalem Account auf dem Mail-Server E-Mails empfangen können. Außerdem werden z. B. `benutzer1@einedomain.example` und `benutzer1@anderedomain.example` dem gleichen lokalen Benutzer `benutzer1` zugeordnet. Dies ist nur bei kleinen Servern praktikabel. In diesem Fall ist es aber auch mit sehr wenig Aufwand verbunden, da keine zusätzliche Benutzerdatenbank gepflegt werden muss.

Relay-Domains

- `relay_domains` legt fest, für welche Domains der Server E-Mails als Backup-MX empfängt
- E-Mails werden nicht lokal gespeichert, sondern an den Haupt-MX weitergeleitet
- wenn dieser nicht erreichbar ist, werden sie zwischengespeichert
- Über `relay_recipient_maps` wird festgelegt, welche Adressen weitergeleitet werden
- über `transport_maps` werden die Server, an die die E-Mails weitergeleitet werden sollen festgelegt

Siehe „Configuring Postfix as primary or backup MX host for a remote site“ in `/usr/share/doc/postfix/STANDARD_CONFIGURATION_README.gz` für weitere Informationen. Diese Datei ist im Paket `postfix-doc` enthalten.

Virtuelle Domains

- bei hosted Domains, deren Adressen keinen lokalen Benutzern entsprechen
- gleiche Adressen unter verschiedenen Domains entsprechen nicht dem gleichen Benutzer
- `virtual_alias_domains`: Adressen haben keine lokalen Mailboxen, sondern werden nur weitergeleitet (evtl. an lokale Benutzer)
- `virtual_mailbox_domains`: Adressen haben lokale Mailboxen

Virtuelle Domains sind bei größeren Mailservern sinnvoll, die viele unabhängige Domains beherbergen. Weitere Informationen dazu finden sich in `/usr/share/doc/postfix/VIRTUAL_README.gz`.

Lab 12.1: Mails von außen annehmen

- Postfix Mails für Test-Domain von außen annehmen lassen
- an lokale User zustellen
- mit `telnet` von Partner-Rechner testen

Dovecot

- POP3- und IMAP-Server
- gute Integration mit Postfix
- kann auch zur Authentifikation von Clients verwendet werden
- Authentifikation standardmäßig über PAM
- kann Mailboxen lokaler Benutzer über POP3/IMAP bereitstellen
- oder virtuelle Mailboxen mit Benutzern in Datenbank

Da Dovecot standardmäßig PAM zur Authentifikation verwendet, kann er nach der Installation direkt verwendet werden um auf die Postfächer lokaler Benutzer zuzugreifen.

Es können aber auch größere Szenarien in Zusammenarbeit mit Postfix Virtual Domains realisiert werden.

Dovecot verfügt über eine umfangreiche Dokumentation unter `http://wiki2.dovecot.org/`.

Dovecot-Installation

- Core: Debian-Paket `dovecot-core`
- POP3: `dovecot-pop3d`
- IMAP: `dovecot-imapd`
- evtl. weitere Pakete für Datenbank-Zugriff

Dovecot-Konfiguration

- Mailbox-Zugriff für lokale Benutzer standardmäßig aktiviert
- Snakeoil-SSL-Zertifikat
- Konfigurations-Dateien unter `/etc/dovecot/` (hauptsächlich im Unter-Verzeichnis `conf.d/`)

Postfix-Authentifikation

- Clients können sich über SASL gegenüber Postfix authentifizieren[1]
- SASL: Simple Authentication and Security Layer, gemeinsames Authentifizierungs-Framework vieler Protokolle
- Postfix benötigt zur Authentifizierung ein SASL-Plugin
- SASL-Plugin z. B. von Dovecot bereitgestellt
- sollte nur über TLS verwendet werden

[1] Jaja

Sollen Mail-Clients außerhalb der in `mynetworks` angegebenen Adressbereiche Mails über den Server versenden können, müssen sie sich authentifizieren. Postfix greift zu Authentifikation auf Plugins zurück. Zweckmäßig ist hier die Verwendung des von Dovecot bereitgestellten Plugins, da Dovecot ohnehin schon Zugriff auf die Benutzerdatenbank hat.

Um das Ausspionieren von Passwörtern zu verhindern, sollte Authentifikation ausschließlich über TLS stattfinden.

Authentifikation: Postfix main.cf

```
1  smtpd_tls_auth_only = yes
2
3  smtpd_sasl_auth_enable = yes
4  smtpd_sasl_type = dovecot
5  smtpd_sasl_path = private/auth
6  smtpd_sasl_security_options = noanonymous
7  smtpd_sasl_authenticated_header = yes
8
9  smtpd_recipient_restrictions =
10   permit_mynetworks,
11   permit_sasl_authenticated,
12   reject_unauth_destination
```


Die Folie enthält den für die Authentifikation zuständigen Teil der Datei `/etc/postfix/main.cf`.

Mit `smtpd_tls_auth_only` wird die Authentifikation ohne TLS deaktiviert. Postfix bietet Clients damit erst eine Authentifikationsmöglichkeit an, wenn diese über STARTTLS eine verschlüsselte Verbindung hergestellt haben.

Mit `smtpd_sasl_auth_enable` wird die Authentifikation über SASL aktiviert.

`smtpd_sasl_type` legt das verwendete Plugin fest, in diesem Fall Dovecot.

`smtpd_sasl_path` legt den Pfad zur Unix-Socket-Datei fest, über die Postfix mit Dovecot kommuniziert. Dieser Pfad ist üblicherweise relativ zum Postfix-Queue-Verzeichnis (Standard: `/var/spool/postfix`) und findet sich in der Dovecot-Konfiguration wieder.

Mit `smtpd_sasl_security_options = noanonymous` wird die anonyme Authentifizierung (entspricht keiner Authentifizierung) deaktiviert.

Mit `smtpd_sasl_authenticated_header` kann festgelegt werden, ob der Benutzername, mit dem sich der Benutzer authentifiziert hat, im Mailheader festgehalten wird. Dies kann bei der Rückverfolgung von Missbrauch nützlich sein.

`smtpd_recipient_restrictions` legt fest, dass neben trusted Clients (`permit_mynetworks`) nun auch authentifizierte Clients den Server als Relay verwenden dürfen (`permit_sasl_authenticated`). Andere Clients dürfen nur E-Mails an lokale Adressen über den Server versenden (`reject_unauth_destination`).

Authentifikation: Dovecot

- in `/etc/dovecot/conf.d/10-master.conf` im Block `service auth`

```
# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
  mode = 0600
  user = postfix
  group = postfix
}
```


Diese Folie enthält den Dovecot-spezifischen Teil der Konfiguration. Es wird hier lediglich ein Unix-Socket bereitgestellt, über den Postfix mit Dovecot kommunizieren kann. Der Pfad `/var/spool/postfix/private/auth` entspricht `smtpd_sasl_path` aus der `main.cf`.

smtptest

- Programm zum Testen von SMTP-Servern
- im Debian-Paket `cyrus-clients-2.4`
- unterstützt TLS und Authentifikation
- `smtptest -t "" -p 25 -a <username> -u <username> mailserver.example.com`
- verbindet sich auf Port 25 zum SMTP-Server und authentifiziert sich mit dem angegebenen Benutzernamen
- verwendet STARTTLS

`smtptest` ermöglicht das Testen von Mail-Servern. Im Gegensatz zu `telnet` ist auch STARTTLS und Authentifizierung möglich.

Der Benutzername muss tatsächlich zweimal angegeben werden, da SASL eine sog. Proxy-Authorisierung unterstützt, mit der ein Benutzer nach der Anmeldung die Identität eines anderen Benutzers annehmen kann.

Nach erfolgreicher Authentifikation kann ein normaler SMTP-Dialog beginnend mit `MAIL FROM` abgewickelt werden.

Lab 12.2: Dovecot

- Dovecot installieren
- IMAP/POP3 testen
- SMTP-Authentifikation einrichten
- Mail per `smtptest` versenden