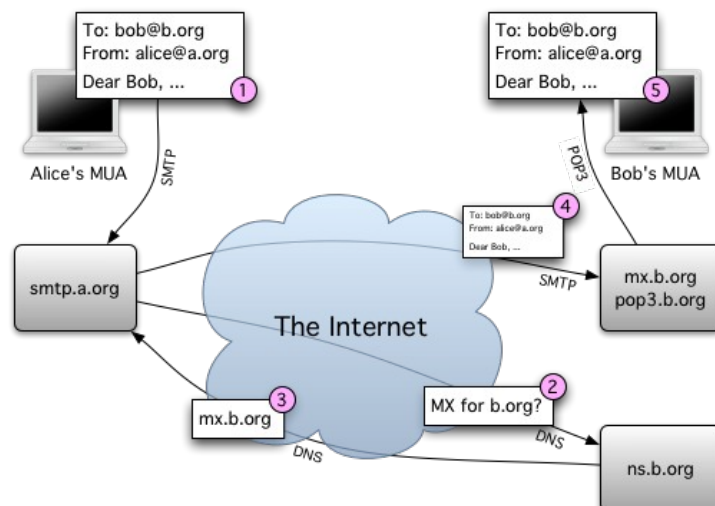


Linux jako mail server

- chování definuje RFC (Request For Comments)
 - RFC 2822 (SMTP)
 - RFC 2045 – RFC 2049 (MIME)
 - a další ...
- „mailserver“ je typicky scénář pro několik úkolů
 - mail relay
 - road-warriors
 - příjem emailů
 - filtrování
 - spam
 - viry
 - přístupy uživatelů
 - schránky
 - webmail

Mail relay

- každá linuxová instalace v podstatě obsahuje MTA



- MTA (Mail Transfer Agent), používá defaultní cron a další služby
- několik obvyklých typů použití
 - internet site
 - smarthost
 - satellite
 - local only



Postfix

- napsal Wietse Venema jako alternativu k dříve dostupným MTA („unixový“ sendmail, „ultimátní“ qmail, ...)
- postaven na konceptu několika daemonů komunikujících mezi sebou
 - rychlý
 - mocný
 - jednoduchý na správu
 - bezpečný
- výborná dokumentace na <http://www.postfix.org>
- velké množství různých podpůrných materiálů různě na webu
- instalace v Debianu: balíček `postfix`
 - pozor na defaultní `exim`
- úvodní konfigurační dialog lze vyvolat příkazem `dpkg-reconfigure postfix`

- v současné době používaná verze 2.2 (Debian „Sarge“), 2.3 (Debian „Etch“)
- konfigurační soubory v `/etc/postfix/`
 - `main.cf`
 - `master.cf`
 - `*.db`
 - „univerzální“ `/etc/aliases` a `newaliases`
- `/etc/aliases`
 - expanze při lokálním doručování

```
# /etc/aliases
mailer-daemon: postmaster
postmaster: root
...
root: Ondrej@cecak.cz
```

`newaliases`

- `/etc/postfix/main.cf`
 - hlavní konfigurační soubor, obvykle obsahuje většinu nastavení pro Postfix
- `/etc/postfix/master.cf`
 - konfigurační soubor jednotlivých daemonů
- `/etc/postfix/*.db`
 - různé mapy (BerkeleyDB), např. `virtual.db`
 - `postmap`

- logy
 - /var/log/syslog
 - /var/log/mail.log
 - /var/log/mail.info
 - /var/log/mail.warn
 - /var/log/mail.err

`/etc/postfix/main.cf`

- myhostname
 - **poštovní jméno**
- mydestination
 - **kam lokálně doručovat**
- relayhost
 - **smarthost**
- mynetworks
 - **kdo má možnost relay (aby náš server nebyl openrelay)**
- inet_interfaces
 - **na které adrese „poslouchat“**
- home_mailbox = Maildir/
 - **doručování do uživatelských adresářů, co email to soubor**

- `/etc/init.d/postfix start/stop/reload`

- `virtual_transport = virtual`
- `virtual_alias_domains = domena.cz`
- `virtual_alias_maps = hash:/etc/postfix/virtual`

```

## domena.cz
#
# systemove aliasy
root@domena.cz          root
postmaster@domena.cz    postmaster
abuse@domena.cz         abuse
#
# ucty
pepa@domena.cz          pepa
jana@domena.cz          jana
@domena.cz              kos
#
# aliasy
pepa.novak@domena.cz    pepa@domena.cz
info@domena.cz          jana

```

- `postmap /etc/postfix/virtual`

```

Feb 23 07:31:59 mail postfix/local[3134]:
C96AF3867B05: to=<pepa@mail.domena.cz>,
orig_to=<info@domena.cz>, relay=local, delay=0,
status=sent (delivered to maildir)

```

```

pepa@mail.domena.cz ... lokální uživatel
info@domena.cz ... alias (často uveden ve FROM:)
C96AF3867B05 ... queue ID

```

- užitečné nástroje
 - `mailq`
 - `postqueue`
 - `postqueue -f`
 - `postsuper`
 - `postsuper -d ALL`

A zpět k mail relay

- SMTP relay pro vnitřní síť
 - pozor na formality v DNS, blacklisty
 - `delay_warning_time = 4h`
 - po 4 hodinách pošle varování odesílateli
 - `maximal_queue_lifetime = 5d`
 - životnost emailu ve frontě 5 dní (implicitní)

Ověření pomocí telnetu

```
$ telnet mail 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.domena.cz ESMTP Postfix
HELO pepa
250 mail.domena.cz
MAIL FROM: <ondrej@cecak.cz>
250 Ok
RCPT TO: <pepa@domena.cz>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
FROM: <ondrej@cecak.cz>
Subject: Pokus

Toto je pokus.
.
250 Ok: queued as CE2984C0B9
QUIT
221 Bye
Connection closed by foreign host.
```

- HELO/EHLO ... definuje standard, úvod komunikace
- MAIL FROM: ... obálkový odesílatel
- RCPT TO: ... příjemce
- DATA ... bude následovat předání emailu
- FROM: ... hlavičkový odesílatel
- prázdný řádek ... odděluje hlavičku od těla emailu
- konec emailu (pokud je součástí emailu tečka na samostatném řádku, escapuje se další tečkou)
- CE2984C0B9 ... queue ID (slouží pro jednoznačnou identifikaci emailu)

Pár doporučení k internet site SMTP

- `unknown_local_recipient_reject_code = 550`
 - odmítat pemanentně lokálně nedoručitelné emaily
- `smtpd_helo_required = yes`
 - vyžadovat HELO/EHLO
- `strict_rfc821_envelopes = yes`
 - striktní kontrola obálkových adres
- `smtpd_sender_restrictions = reject_unknown_sender_domain`
 - jednoduchá kontrola odesílatele emailu – uvedená doména musí být platná
- jednotlivé uživatele zakládat odděleně od ostatních a neumožnit jim lokální přihlášení
 - `/etc/passwd`
`pepa:x:1026:1026:Josef Novak,,,,email`
`only:/home/mail/pepa:/bin/true`

Přístup k emailům pro uživatele

- oblíbené a používané především tři metody
 - POP3
 - IMAP (IMAP4)
 - webmail

POP3, IMAP

- protokoly, kterým komunikuje uživatelské MUA (Mail User Agent)

Dovecot



- podobně jako Postfix mladý
- napsán s ohledem na bezpečnost a spolehlivost
- dokumentace ve wiki na <http://www.dovecot.org>

- instalace v Debianu
 - `aptitude install dovecot`
- konfigurační soubory
 - `/etc/dovecot/`
 - `/etc/dovecot/dovecot.conf`
 - `/etc/init.d/dovecot start/stop`
- logy
 - stejně jako Postfix, tedy mimo jiné:
 - `/var/log/mail.log`

- `/etc/dovecot/dovecot.conf`
 - `protocols = imap imaps pop3s`
 - aktivní protokoly
 - certifikát X.509 (SSL/TLS) má výchozí
 - `imap_listen = localhost`
 - IMAP pouze lokálně kvůli webmailu

Feb 24 08:55:53 mail imap-login: Login: pepa
[83.49.267.269]



Webmail – SquirrelMail

- jednoduchý webový klient v PHP
 - čistý
 - bezpečný
 - dokumentace na <http://www.squirrelmail.org/>
- instalace v Debianu
 - `aptitude install squirrelmail`
- interaktivní konfigurace
 - `squirrelmail-configure`
- vyžaduje webový server

Další užitečné programy

- obecný filtr `amavisd-new`
- spamfilter `spamassassin`
- antivirus `ClamAV`

Fetchmail a doménové koše

- fetchmail vybírá POP3 schránku na serveru a předává lokálnímu MTA na port 25 (tj. jako by emaily byly doručeny „standardně“)
- instalace v Debianu:
 - `aptitude install fetchmail`
- spouštění např. periodicky cronem
 - `fetchmail >>`
`/var/log/fetchmail.log 2>&1`
- konfigurace:
 - `/root/.fetchmailrc`

```
poll mail.domena.cz proto pop3
  localdomains domena.cz
  envelope "Received"
  envelope "To"
  envelope "Cc"
  envelope "Bcc"
  envelope "Envelope-To"
  user "user" password "secret" to * here
```

- třídící pravidlo pro doručování je určeno proměnnou `envelope`