Elektronicka posta - jednoduche zaklady

Jiri Kubina

jiri.kubina@osu.cz

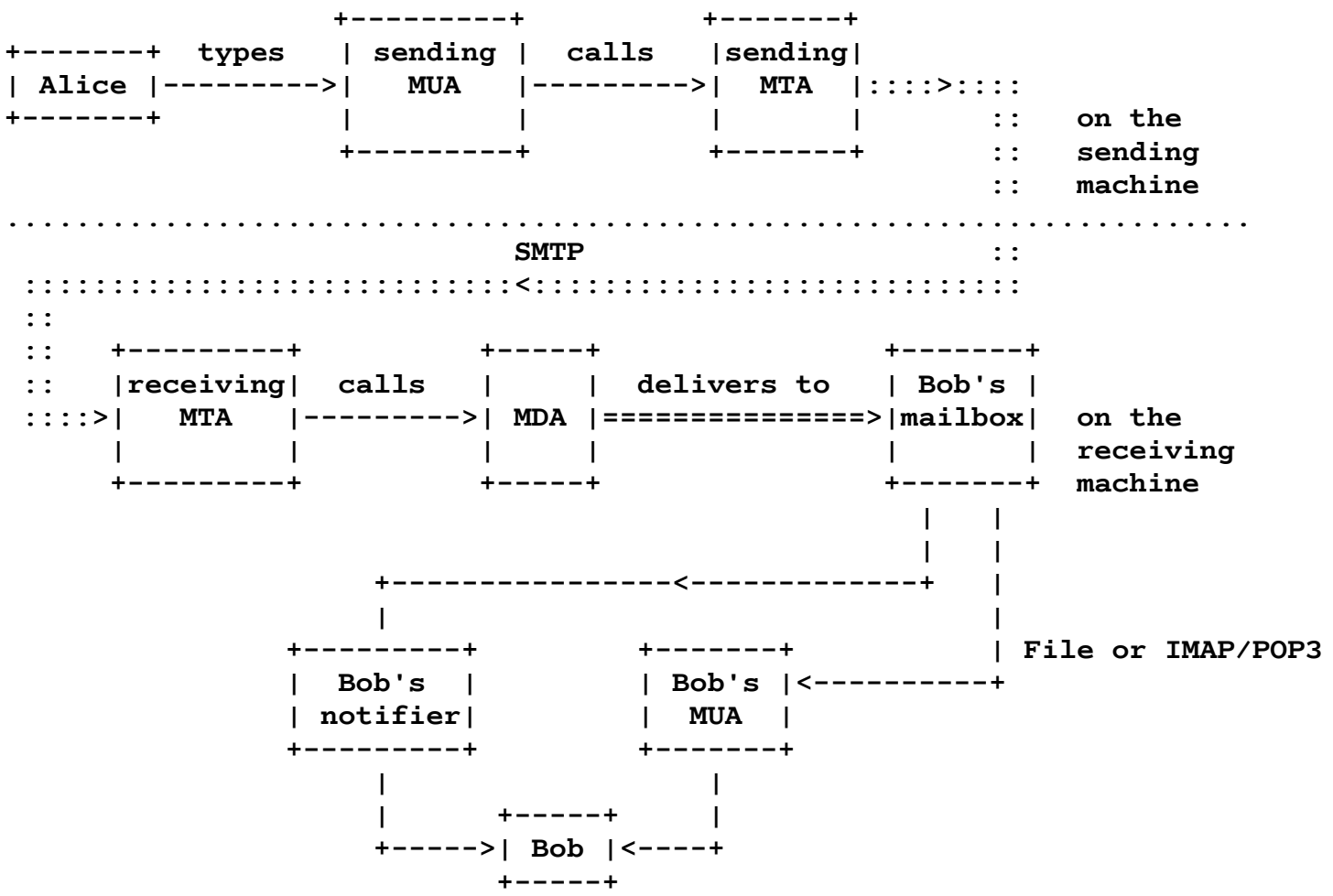
Ver. 1.0

leden 2006

Obsah

Upozorneni: Vetsina popisovanych principu je zjednodusena, nebo zkracena z vyukovych duvodu. Pro ziskani kompletnich informaci ctete RFC.

1.Jak putuje email



2.MTA,MUA,MDA

MTA - Mail Transport Agent

Programy pouzivane jako mail transport agent:

- Sendmail
- Postfix
- Exim
- Qmail
- Exchange

Protokol pro komunikaci mezi MTA: **SMTP**

MUA - Mail User Agent

Programy pouzivane jako mail user agent:

- Mail
- Pine
- Mutt
- Thunderbird
- Evolution
- Outlook

Pristupove metody **MUA** do emailove schranky:

- soubory /lokalni nebo na sitovem souborovem systemu/
- POP3
- IMAP

MDA - Mail Delivery Agent

- **MTA** - dorucuje postu pouze mezi dvema mail servery
- **MDA** - dorucuje postu do uzivatelskych mailboxu
- **MDA** - muze byt pouzit k automatickym odpovedim nebo filtrovani posty

Programy pouzivane jako MDA :

- procmail
- maildrop

3.SMTP – strucne

SMTP - Simple Mail Transfer Protocol

- Jednoduchy protokol ve kterem jsou jednotlive prikazy posilany jako text v ASCII
- Snadno realizovatelne odeslani mailu pomoci programu Telnet
- TCP port 25

Priklad odeslani mailu pomoci programu Telnet

```
jura@moby:~> telnet 10.2.3.168 25
Trying 10.2.3.168...
Connected to 10.2.3.168.
Escape character is '^]'.
220 neo.firma1.intr ESMTP Postfix
MAIL FROM:nekdo@firma1.intr
250 Ok
RCPT TO:jura@firma1.intr
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
jak se vam dari ?
.
250 Ok: queued as 970EB3B4086
QUIT
221 Bye
Connection closed by foreign host.
```

SMTP prikazy

HELO klient	Klient se predstavuje serveru jmenem pocitace.
MAIL FROM:	Odesilatel
RCPT TO:	Prijemce
DATA	Telo zpravy
RSET	Reset. Dosud zadane informace FROM a TO budou zahozeny.
VRFY adresa	Dotaz zda server zna uvedenou adresu.
QUIT	Ukonceni spojeni

ESMTP - Extension Simple Mail Transfer Protocol

- Rozsireni protokolu SMTP, pri zachovani zpetne kompatibility.
- Klient, aby zvolil spravnou sadu prikazu musi rozpoznat zda server podporuje SMTP nebo ESMTP. Dela to prikazem EHLO /pokud na tento prikaz obdrzi klient kod 250 vi ze server je ESMTP, jinak jej povazuje za SMTP/.
- RFC-1869.

Priklad rozpoznani ESMTP serveru

```
jura@moby:~> telnet 10.2.3.168 25
Trying 10.2.3.168...
Connected to 10.2.3.168.
Escape character is '^]'.
220 neo.firma1.intr ESMTP Postfix
EHLO 10.2.3.167
250-neo.firma1.intr
250-PIPELINING
250-SIZE 20971520
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH CRAM-MD5 GSSAPI DIGEST-MD5 NTLM LOGIN PLAIN
250-AUTH=CRAM-MD5 GSSAPI DIGEST-MD5 NTLM LOGIN PLAIN
250 8BITMIME
```

4.POP3 – strucne

POP3 - Post Office Protocol ver. 3

- Jednoduchy protokol umoznujici uzivateli stahnout ze serveru zpravy do lokalni postovni schranky na svem PC
- Offline prace
- Spojeni se sklada ze dvou stadii:
  - Autentizacni stav
  - Transakcni stav
- Prikazy protokolu jsou textove v ASCII
- RFC-1939
- TCP port 110
- Zabezpecena varianta – POP3S TCP port 995
- Zabezpecenou variantu lze testovat z prikazoveho radku pomoci OpenSSL klienta:

openssl s_client -host 10.2.3.168 -port 995

Priklad komunikace s POP3 serverem pomoci programu Telnet

```
jura@moby:~> telnet 10.2.3.168 110
Trying 10.2.3.168...
Connected to 10.2.3.168.
Escape character is '^]'.
+OK dovecot ready.
USER jura
+OK
PASS heslo
+OK Logged in.
STAT
+OK 1 969
LIST
+OK 1 messages:
1 969
.
RETR 1
+OK 969 octets
Return-Path: <jura@firma1.intr>
X-Original-To: jura@firma1.intr
Delivered-To: jura@firma1.intr
Received: from [10.2.3.168] (neo.firma1.intr [10.2.3.168])
        (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by neo.firma1.intr (Postfix) with ESMTP id E62233B4086
        for <jura@firma1.intr>; Wed,  1 Feb 2006 12:52:24 +0100 (CET)
Message-ID: <43E0A0F8.4010309@firma1.intr>
Date: Wed, 01 Feb 2006 12:52:24 +0100
```

```
From: jura1 <jura@firma1.intr>
User-Agent: Mozilla Thunderbird 1.0.7-1.4.1.centos4 (X11/20051007)
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: jura@firma1.intr
Subject: mailik
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit
X-IMAPbase: 1138266105 21
Status: O
X-UID: 21
Content-Length: 31
X-Keywords:

hgfhjgfhgfhjgh
hgdfhgdfhjgdjgh
.
DELE 1
+OK Marked to be deleted.
RSET
+OK
QUIT
+OK Logging out.
Connection closed by foreign host.
```

POP3 prikazy

USER name	Uzivatelske jmeno
PASS password	Heslo
STAT	Pocet zprav ve schrance a celkovou velikost zprav
LIST	Seznam jednotlivych zprav a jejich velikosti
RETR cislo	Stahne zpravu /jejiz cislo je parametr prikazu/ ze serveru ke klientovi
DELE cislo	Smaze zpravu /jejiz cislo je parametr prikazu/.
RSET	Obnovi zpravy smazane v prubehu aktualni relace.
TOP cislo radek	Vypise pocatek zpravy od udaneho radku.
QUIT	Ukonci spojeni. V tomto okamziku se smazou vsechny zpravy oznacene prikazem DELE

5.IMAP – strucne

IMAP4 - Internet Message Access Protocol ver. 4

- Sofistikovany protokol pro praci s postovnimi schrankami.
- Umoznuje pracovat se schrankou vice aplikacim najednou.
- Online i Offline prace
- TCP port 143
- Testovani pomoci Telnetu je mozne, je však slozitejsi nez v pripade POP3.
- Zabezpecena varianta - IMAPS TCP port 993
- Zabezpecenou variantu lze testovat z prikazoveho radku pomoci OpenSSL klienta:

- **openssl s_client -host 10.2.3.168 -port 993**

6.Postfix

Vykonna, bezpecna a snadno konfigurovatelna alternativa k postovnimu systemu sendmail, ktery je dosud povazovan za Linux/Unix standart.

Zakladni principy Postfixu :

- jednoduchost
- modularnost
- bezpecnost

Postfix se narozdil od jinych systemu /typicky sendmail/, ktere funguji jako jeden proces zajistujici prijimani i odesilani posty, sklada z nekolika modulu, ktere provadeji jednu presne specifikovanou cinnost.

Postfix je implementovany jako jeden hlavni proces "**master**", ktery spousti obsluzne demony vykonavajici specificke ukony podle potreby.

Daemony Postfixu

smtpd	posloucha na portu a prijima SMTP pozadavky. Vsechny prijate zpravy jsou presmerovane na daemona "cleanup"
pickup	ceka na lokalne napsane maily a smeruje je na daemona "cleanup"
cleanup	spracovava prijaty mail (pridava chybejici hlavicky atd.), dava ho do fronty prijatych mailu a informuje daemona "qmgr" o jeho prichodu
qmgr	ceka na prijate maily a zajistuje jejich doruceni. Zpusob doruceni urci daemon "trivial-rewrite"
trivial-rewrite	prepisuje adresu do standartni formy. Pripojuje jmeno domeny k lokalnim mailum ktere ji nemaji uvedenou a pod. Krome toho urcuje co se stane s mailem, jak a kam se bude dorucovat na zaklade adresy.
local	dorucuje mail do lokalnich chranek na serveru

smtp smtp klient Postfixu. Dorucuje maily z mailove fronty, ktere jsou urcene pro jine mailove servery

Minimalni konfigurace Postfixu

Soubor /etc/postfix/main.cf

```
myhostname = neo.firma1.intr
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = firma1.intr
mydestination = $myorigin,$myhostname,
                  localhost.localdomain, localhost
mynetworks = 127.0.0.0/8
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
inet_interfaces = all
```

Zakladni konfiguracni nastaveni /etc/postfix/main.cf

myhostname = neo.firma.intr
urcuje cele jmeno serveru. Standardne se pouzije jmeno serveru zjistene z operacniho systemu (hostname)

alias_maps = hash:/etc/aliases
umisteni a tvar aliasove mapy. Postfix prijme mail pro neexistujiciho uzivatele a doruci ji uzivateli ktery je uveden u tohoto aliasu.

alias_database = hash:/etc/aliases
umisteni databaze aliasu, kterou vytvori prikaz newaliases ze souboru uvedeneho u alias_maps. /typ hash na priponu .db/

myorigin = firma1.intr
urcuje jmeno serveru v odchazejici poste z tohto serveru

mydestination = $myhostname, $mydomain, localhost.localdomain, localhost
domenove adresy, ktere Postfix povazuje za lokalni a pro ktere prijima postu. Pokud spatne nastavite tuto promennou, mailov server nebude prijimat postu

mynetworks = 127.0.0.0/8

adresy klientskch pocitacu, ktere muzou pomoci Postfixu odesilat postu (pomocou SMTP). Pokud nespravne nastavite tuto promennou, Postfix neumozni klientum posilat postu (odmitne pripojeni)

mailbox_command = procmail -a "$EXTENSION"

dorucovani posty do lokalnich mailboxu pomoci programu "procmail"

mailbox_size_limit = 104857600

omezeni velikosti mailboxu na 100MB /0=neomezeno/

inet_interfaces = all

seznam adres (ne eth0) sitovych rozhrani na kterych se prijima posta

7.Dovecot

Dovecot je open source **IMAP/POP3** server urceny pro Linux/UNIX-like systemy. Umi pracovat s obema standartnimi formaty schranek mbox i maildir. Obsahuje samozrejme kompletni podporu zabezpeceneho prenosu TLS/SSL.

Minimalni konfigurace Dovecot /etc/dovecot.conf

```
protocols = imap pop3 imaps pop3s
imap_listen = *
pop3_listen = *
imaps_listen = *
pop3s_listen = *
ssl_cert_file = /etc/postfix/ssl/smtpd.crt
ssl_key_file = /etc/postfix/ssl/smtpd.key
login_dir = /var/run/dovecot-login
login = imap
login = pop3
mbox_locks = fcntl
auth = default
auth_mechanisms = plain
auth_userdb = passwd
auth_passdb = pam
auth_user = root
```

8.Postfix+SASL+TLS+Dovecot

Ukazka komlexni konfigurace Postfix s uzivatelskou autentifikaci **SASL** a zabezpecenym prenosem dat **TLS**, vcetne konfigurace **Dovecot IMAP/POP3** serveru se zabezpecenymi variantami techto sluzeb **IMAPS/POP3S.**

Funkcni konfigurace /CentOS 4.2/

1. vypnout SELinux
/etc/sysconfig/selinux
SELINUX=disabled

2. vypnout IPv6 /neni nutne/
/etc/modprobe.conf pridat na konec alias net-pf-10 off

3. rozjet si korektni MX dns zaznam pro zvolenou domenu
dig -t mx firma1.intr

```
; <<>> DiG 9.2.4 <<>> -t mx firma1.intr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46174
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
```

```
;; QUESTION SECTION:
;firma1.intr.                   IN      MX

;; ANSWER SECTION:
firma1.intr.            38400   IN      MX      10 neo.firma1.intr.

;; AUTHORITY SECTION:
firma1.intr.            38400   IN      NS      neo.

;; ADDITIONAL SECTION:
neo.firma1.intr.        38400   IN      A       195.113.106.168

;; Query time: 0 msec
;; SERVER: 195.113.106.168#53(195.113.106.168)
;; WHEN: Thu Jan 26 13:10:15 2006
;; MSG SIZE  rcvd: 82

4. instalace potrebnych baliku
    yum install postfix postfix-pflogsumm dovecot cyrus-sasl cyrus-sasl-devel
cyrus-sasl-gssapi cyrus-sasl-md5 cyrus-sasl-ntlm cyrus-sasl-plain

5. odinstalace sendmailu
    yum remove sendmail

6. konfigurace postfixu

----standartni cast----
myhostname = neo.firma1.intr
mydomain = firma1.intr
myorigin = $mydomain
```

```
inet_interfaces = $myhostname, localhost
mydestination = $myhostname, $mydomain, localhost
local_recipient_maps = unix:passwd.byname $alias_maps
unknown_local_recipient_reject_code = 550
mynetworks_style = subnet
mynetworks = 195.113.106.0/24, 127.0.0.0/8
relay_domains = $mydestination
mail_spool_directory = /var/spool/mail

----sasl cast----
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks,
reject_unauth_destination

----omezeni velikosti prilohy a schranky----
message_size_limit = 20971520
mailbox_size_limit = 104857600

----TLS cast----
smtpd_tls_auth_only = no
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
```

```
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

7. konfigurace dovecot

protocols = imap pop3 imaps pop3s
imap_listen = *
pop3_listen = *
imaps_listen = *
pop3s_listen = *
ssl_cert_file = /etc/postfix/ssl/smtpd.crt
ssl_key_file = /etc/postfix/ssl/smtpd.key

8. konfigurace saslauthd /kontrola/
    /usr/lib/sasl2/smtpd.conf
    pwcheck_method: saslauthd

9. nastaveni postfixu jako MTA /kontrola/
    alternatives --config mta /na prikazovem radku/


10.generovani klice a certifikatu pro TLS v postfixu
    mkdir /etc/postfix/ssl
    cd /etc/postfix/ssl/

    openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024

    <- zadejte heslo pro smtpd.key

    chmod 600 smtpd.key
```

```
openssl req -new -key smtpd.key -out smtpd.csr

<- Zadejte heslo pro smtpd.key
<- Zkratka zeme ("CZ")
<- Nazev statu ("Czech Republic")
<- Mesto
<- Nazev organizace
<- FQDN ("mail.domena.tld")
<- Emailova@adresa.tld Dalsi informace jsou volitelne

openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt

<- zadejte heslo pro smtpd.key

openssl rsa -in smtpd.key -out smtpd.key.unencrypted

Zadejte heslo pro smtpd.key.

mv -f smtpd.key.unencrypted smtpd.key

openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem
-days 3650

<- Zadejte heslo pro smtpd.key
<- Zkratka zeme ("CZ")
<- Nazev statu ("Czech Republic")
<- Mesto
<- Nazev organizace
<- FQDN ("mail.domena.tld")
<- emailova@adresa.tld
```

11.restartovani prekonfigurovanych services

```
/etc/init.d/saslauthd restart
/etc/init.d/postfix restart
/etc/init.d/dovecot restart
```

12.kontrola spousteni service pri bootu systemu

```
chkconfig --list saslauth
chkconfig --list postfix
chkconfig --list dovecot
```

13.kontrola funkcionality smtp serveru

```
[root@neo /]#telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 neo.firma1.intr ESMTP Postfix
ehlo localhost
250-neo.firma1.intr
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH CRAM-MD5 GSSAPI DIGEST-MD5 NTLM LOGIN PLAIN
250-AUTH=CRAM-MD5 GSSAPI DIGEST-MD5 NTLM LOGIN PLAIN
250 8BITMIME
```

Pokud vidime moznost STARTTLS a radky zacinajici AUTH je vse ok.

9.Pouzite zdroje a nastroje

Zdroje

- Velky pruvodce protokoly TCP/IP a systemem DNS - L.Dostalek, A.Kabelova
- Velky pruvodce protokoly TCP/IP Bezpecnost – L.Dostalek a kolektiv
- V prezentaci je pouzit obrazek z http://www.tldp.org/HOWTO/Mail-Administrator-HOWTO.html
- www.postfix.org
- www.dovecot.org
- www.abclinuxu.cz

Nastroje

- telnet

Dekuji za pozornost