

OpenSMTPD over the clouds

the story of an HA setup

Giovanni Bechis
<giovanni@openbsd.org>

Fosdem 2020, Brussels

SN3

Information Technology
& Web Solutions



Historical setup

- ▶ some OpenBSD mail servers
- ▶ Postfix + Apache SpamAssassin + Amavisd-new + Courier Imap
- ▶ no shared storage
- ▶ no load balancer

fixed pieces of the puzzle

- ▶ OpenBSD
- ▶ Apache SpamAssassin

first steps towards smtpd(8)



- ▶ customers started sending marketing newsletters via the primary mail server
- ▶ some dedicated smtpd(8) mail servers to send out newsletters

[smtpd(8)] web gui

The screenshot displays the ISPConfig web interface. At the top, the header includes the logo 'ISPConfig' and the text 'hosting control panel'. On the right side of the header, there is a 'LOGOUT ADMIN' link and a search bar. Below the header is a navigation bar with icons for Home, System, Client, DNS, Help, Email (which is highlighted), Monitor, Sites, and Tools. A left sidebar contains a menu with categories: Email Accounts, Mailing List, Spamfilter, Fetchmail, and Statistics. The main content area is titled 'Mailbox' and features four tabs: Mailbox (selected), Autoresponder, Mail Filter, and Custom Rules. The configuration form includes fields for Name (Optional), Email (with sub-fields for Alias 'giovanni' and Domain 'giovanni.it'), Password (with a 'Generate Password' link), Password strength, Repeat Password, Quota (1000 MB), Send copy to (Optional), Spamfilter (Normal), Enable Receiving (checked), Disable IMAP, and Disable POP3.

ISPConfig
hosting control panel

LOGOUT ADMIN

Search

Home System Client DNS Help **Email** Monitor Sites Tools

Email Accounts

- Domain
- Domain Alias
- Email Mailbox
- Email Alias
- Email Forward
- Email Catchall
- Email Routing

Mailing List

- Mailing List

Spamfilter

- Whitelist
- Blacklist
- User / Domain
- Policy

Fetchmail

- Fetchmail

Statistics

- Mailbox quota
- Mailbox traffic

Mailbox Autoresponder Mail Filter Custom Rules

Name (Optional)

Email * Alias Domain

Password [Generate Password](#)

Password strength

Repeat Password

Quota (0 for unlimited) MB

Send copy to (Optional)

Spamfilter

Enable Receiving

Disable IMAP

Disable POP3

HA mail server setup

- ▶ pf(4) and relayd(8)
- ▶ shared nfs storage
- ▶ MySQL master-master replica to share databases (users, addressbooks, calendars, ...)

[relayd(8)] HA mail server setup

```
mx0_pub="1.2.3.4"  
mx0_priv="10.0.0.4"  
mx1_priv="10.0.0.5"  
  
table <mx0> { $mx0_priv }  
table <fallback-mx0> { $mx1_priv }  
  
redirect mx0-smtp {  
    listen on $mx0_pub port smtp \  
        interface $if_pub sticky-address  
  
    pftag RELAYD  
  
    forward to <mx0> check tcp  
    forward to <fallback-mx0> check tcp  
}
```

[mysqld(8)] HA mail server setup

```
[mysqld]
server-id      = 1

binlog-do-db  = dbispcnfig
binlog-do-db  = sogo

replicate-do-db = dbispcnfig
replicate-do-db = sogo

auto_increment_increment= 2
auto_increment_offset   = 1
```


[mysqld(8)] HA mail server setup

```
mysql> CHANGE MASTER TO MASTER_HOST='10.0.0.5', \  
MASTER_PORT=3306, MASTER_USER='replica', \  
MASTER_PASSWORD='changeme', \  
MASTER_LOG_FILE='slave-bin.000831', \  
MASTER_LOG_POS=341, MASTER_CONNECT_RETRY=10;  
  
mysql> CHANGE MASTER TO master_use_gtid=slave_pos;
```

[smtpd(8)] mail server setup

```
pki mx.domain.tld cert "/etc/.../fullchain.pem"  
pki mx.domain.tld key "/etc/.../privkey.pem"  
  
table aliases file:/etc/mail/aliases  
  
table vusers mysql:/etc/mail/mysql.conf  
table vdomains mysql:/etc/mail/mysql.conf  
table valiasess mysql:/etc/mail/mysql.conf  
table credentials mysql:/etc/mail/mysql.conf
```

[smtpd(8)] mail server setup

```
host 127.0.0.1
username ispcsrv6
password XXX
database dbispcconfig

# Alias lookup query
query_alias      SELECT destination FROM mail_valias \
                  WHERE source=?

# Domain lookup query
query_domain     SELECT domain FROM mail_domain \
                  WHERE domain=?;

# User lookup query
query_userinfo   SELECT uid,gid,maildir \
                  FROM mail_user WHERE \
                  REPLACE(login, '@', '_')=? \
                  AND server_id=6;

# Credentials lookup query
query_credentials SELECT login, password FROM mail_user \
                  WHERE login=? AND disablesmtp='n';
```

[smtpd(8)] antispam setup

```
filter check_dyndns phase connect match rdns \  
  regex { '.*\.dyn\.*', '.*\.dsl\.*' } \  
  disconnect "550 no residential connections"  
  
filter check_rdns phase connect match !rdns \  
  disconnect "550 no rDNS available"  
  
filter "dkimsign" proc-exec "filter-dkimsign \  
  -d domain.tld -s dkim \  
  -k /etc/mail/dkim/key.pem" \  
  user _dkimsign group _dkimsign  
  
filter "spamassassin" proc-exec "filter-spamassassin"
```

[smtpd(8)] antispam setup

```
listen on socket filter "dkimsign"  
listen on lo0 filter "dkimsign"  
listen on egress filter { check_dyndns, check_rdns, \  
    spamassassin } \  
    tls pki mx.domain.tld  
listen on egress filter { check_dyndns, check_rdns, \  
    spamassassin } \  
    smtps pki mx.domain.tld  
listen on egress port submission filter "dkimsign" \  
    tls auth <credentials> pki mx.domain.tld
```

[smtpd(8)] clamd(8) integration

- ▶ use filter-clamav
- ▶ use SpamAssassin ClamAV plugin

[smtpd(8)] Sender Rewriting Scheme setup

```
srs key "XXX"  
action "outbound" relay srs
```

[smtpd(8)] mail server setup

```
action "deliver_local" mbox alias <aliases>

action "mymda" \
  mda "/usr/local/scripts/mailedrop \
  -w 90 -d vmail '+' %{rcpt:lowercase} \
  %{user.username} %{dest.domain} %{sender}" \
  userbase <vusers> virtual <valiases>

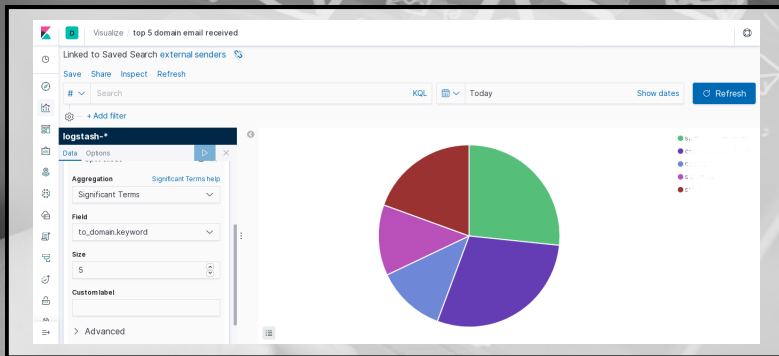
action "outbound" relay srs

match from any for domain <vdomains> action "mymda"
match for local action "deliver_local"
match from auth for any action "outbound"
```


[smtpd(8)] log files

```
smtpd[89374]: f9f470e4d4702127 smtp connected address=199.185.178.25 \  
host=mail.openbsd.org  
smtpd[89374]: f9f470e4d4702127 smtp tls \  
ciphers=TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256  
  
spamd[63035]: spamd: connection from ::1 [::1]:23701 to port 783, fd 5  
spamd[63035]: spamd: processing message \  
<1a13f6ebf7bf3562d49f362f@yourdomain.tld> for (unknown):506  
spamd[60192]: util: setuid: ruid=506 euid=506 rgid=506 506 506 egid=506 \  
506 506  
filter-spamassassin[59437]: f9f470e4d4702127 result \  
Spam: False ; -15.9 / 6.0  
spamd[63035]: spamd: clean message (-15.9/6.0) for (unknown):506 \  
in 2.7 seconds, 3062 bytes.  
spamd[63035]: spamd: result: . -15 - BAYES_00,KAM_DMARC_STATUS, \  
MAILING_LIST_MULTI,RCVD_IN_DNSWL_MED,RCVD_IN_HOSTKARMA_W,\  
SPF_HELO_NONE,TXREP scantime=2.7,\  
size=3062,user=(unknown),uid=506,required_score=6.0,rhost>:::1,raddr>:::1,\  
rport=23701,mid=<1a13f6ebf7bf3562d49f362f@yourdomain.tld>,bayes=0.000000,\  
autolearn=ham autolearn_force=no,shortcircuit=no  
  
smtpd[89374]: f9f470e5b1148f0e mda delivery evpid=94aab3d00b735a11 \  
from=<owner-hackers+M92599=me=mydomain.tld@openbsd.org>  
to=<me@mydomain.tld> \  
rcpt=<me@mydomain.tld> user=me_mydomain.tld delay=3s \  
result=0k stat=Delivered
```

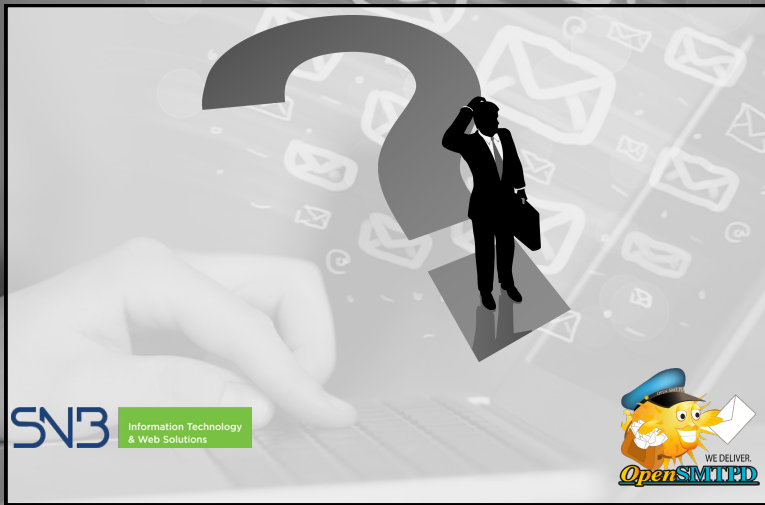
[smtpd(8)] log analysis.



what's missing ?

- ▶ SpamAssassin per-user setup
- ▶ get rid of maildrop wrapper
- ▶ greylisting, maybe
- ▶ relayd(8) setup based on more data

Questions ?



The image shows a hand pointing at a large question mark on a laptop screen. The background is filled with various email icons and symbols, suggesting a focus on digital communication and technology. The overall theme is about asking questions and seeking solutions in the IT and web services industry.

SN3 Information Technology & Web Solutions

OpenSMITD WE DELIVER.