Mail transfer agent (1)

Tykushin Anatoly, a.tykushin@innopolis.ru, MSIT-SNE

September 2016

Contents

1 Installation of MTA

According to the task I was supposed to install ***Sendmail*** as MTA. Running a little ahead I failed this task. In the subsections below I'll try to explain what was the problem and describe followed steps during installation.

1.1 Downloading and verifying sources of MTA

1.1.1 Downloading sources, keys and signatures

This stuff could be done by this commands:

```
wget ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.15.2.tar.gz -- downloading sources
wget ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.15.2.tar.gz.sig -- downloading signature
```

1.1.2 Verifying stage

Verification consists of:

- importing keys and signatures

  ```
  gpg --import sendmail2015.asc
  gpg --verify sendmail.8.15.2.tar.gz.sig
  ```

- verifying signature

  ```
  gpg sendmail.8.15.2.tar.gz.sig  -- command

  gpg: keyring '/home/tyvision/.gnupg/secring.gpg' created
  gpg: keyring '/home/tyvision/.gnupg/pubring.gpg' created
  gpg: assuming signed data in 'sendmail.8.15.2.tar.gz'
  gpg: Signature made Thu 02 Jul 2015 03:39:10 PM MSK using RSA key ID 05BDCC53
  -- here is public key ID
  gpg: Can't check signature: public key not found -- that we have to download
  ```

- getting public key

  ```
  gpg --keyserver pgpkeys.mit.edu --recv-key 05BDCC53 -- command

  gpg: requesting key 05BDCC53 from hkp server pgpkeys.mit.edu
  gpg: /home/tyvision/.gnupg/trustdb.gpg: trustdb created
  gpg: key 05BDCC53: public key "Sendmail Signing Key/2015 <sendmail@Sendmail.ORG>" imported
  gpg: no ultimately trusted keys found
  gpg: Total number processed: 1 -- result of import
  gpg:               imported: 1  (RSA: 1)
  ```

- building a chain of trust

  ```
  gpg --edit-key sendmail@Sendmail.ORG trust -- command

  gpg: checking the trustdb -- output of the command
  .... -- uninformative logs

  <setting option "how far do you trust this user to correctly verify keys">
  -- answer is "I trust ultimately"
  ..  -- uninformative logs
  ```

- verifying signature again

  ```
  gpg sendmail.8.15.2.tar.gz.sig  -- command

  gpg: assuming signed data in 'sendmail.8.15.2.tar.gz'
  gpg: Signature made Thu 02 Jul 2015 03:39:10 PM MSK using RSA key ID 05BDCC53
  gpg: checking the trustdb
  gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
  gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
  gpg: Good signature from "Sendmail Signing Key/2015 <sendmail@Sendmail.ORG>" -- means that
  everything is good
  ```

1.2 Compilation of sources

Compilation failed with many errors. One of them that wasn't able to fix was usage on -DNEWDB flag. Latest version was installed from official ubuntu repository.

2 Setting up DNS zone

2.1 Adding records to zone file

It's required to add **MX** records records to the zone file:

```
MX 10 mail.st5.os3.su. -- server's own MX record
```

2.2 Information for the upper zone

```
st5.os3.su . MX 10 mail.st5.os3.su. -- MX record to the stX mail server
```

3 Basic configuration of MTA

3.1 Adding local user and checking mail delivery

3.1.1 How to add local users

After installation of sendmail from repository, local user account was created in order to what user installed sendmail. For me it was **tyvision**. To enable other local users you can edit file **/etc/mail/local-host-names** and then recompile configuration for sendmail. Example of **/etc/mail/local-host-names file is shown below**

```
    localhost       -- stock
    a.tykushin      -- name of user (edited by myself)
```

3.1.2 Trying to send email to local user

You can see mail sent from my innopolis account to local a.tykushin@st5.os3.su address.

```
------------------------------------------------------------------
            LOGS FROM /var/mail/a.tykushin
------------------------------------------------------------------


Sep 15 23:45:55 st5 sm-mta[3851]: u8FKjscQ003851: from=<a.tykushin@innopolis.ru>, size=2047, class=0, nrc
Sep 15 23:45:55 st5 sm-mta[3852]: u8FKjscQ003851: to=tyvision@st5.os3.su, delay=00:00:00, xdelay=00:00:00


------------------------------------------------------------------
            MESSAGE /var/mail/a.tykushin
------------------------------------------------------------------


    From a.tykushin@innopolis.ru  Thu Sep 15 21:20:21 2016
Return-Path: <a.tykushin@innopolis.ru>
Received: from st3.os3.su (mail.st3.os3.su [188.130.155.36])
by st5.os3.su (8.15.2/8.15.2/Debian-3) with ESMTP id u8FIKJds001719
for <a.tykushin@st5.os3.su>; Thu, 15 Sep 2016 23:2:21 +0300
Received: from smtp.university.innopolis.ru (unknown [10.90.104.83])
by st3.os3.su (Postfix) with ESMTP id 5CFBA36C0551
for <a.tykushin@st5.os3.su>; Thu, 15 Sep 2016 21:17:23 +0300 (MSK)
Content-Language: ru-RU
Content-Type: multipart/alternative;
boundary="_000_36b4ab7cc0584c0487ea409534631c61EXMB02eduinnopolisru_"
DKIM-Signature: v=1; a=rsa-sha256; d=innopolis.ru; s=unimail1;
c=simple/simple; t=1473963422; h=from:subject:to:date:message-id;
bh=BoeJLv6mzBLIH1sWHhYPbR53mwbjk9R2GYbDyPrsO64=;
b=jD1E6VeM7JG3P6EHdKFUqMuzDf5NL6Jshn6H3ToJUouwV48aaH44a7OaVQuRNx2aZO0alRWOwCk
QeFnyss4e4Ky82pH0AxldVqkIQH2PR/duO6408bHcx1ZWQvU+3nRH7ufnL/z/puFHAATgxSPr8Gki
Y6cpecV0l99vBlMhvB2Gr8d4NYxi0nun8x5fELNdq/MKN7LRdLM/uhnKtv1rf5BKpLqSHzWfqra1W
b4yCyR3S0ZmC9YRCPLufpxzI/kGk8C5XMiR3EZBK8rA5KLT140+Y+/AUjHMvbZ1fOF2ErYs8DS61X
sBG9YBavaAIvoh/R3PfAMMwfKjOCJ4WyeJCA==
From: Tykushin Aantoly <a.tykushin@innopolis.ru>
To: "a.tykushin@st5.os3.su" <a.tykushin@st5.os3.su>
Subject: Backup2
Thread-Topic: Backup2
Thread-Index: AQHSD31auZkwNN1KiUCktTHt2HdSBg==
```

```
Date: Thu, 15 Sep 2016 18:17:01 +0000
Message-ID: <36b4ab7cc0584c0487ea409534631c61@EXMB02.edu.innopolis.ru>
Accept-Language: ru-RU, en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
x-ms-exchange-transport-fromentityheader: Hosted
x-originating-ip: [10.90.136.10]
MIME-Version: 1.0


--_000_36b4ab7cc0584c0487ea409534631c61EXMB02eduinnopolisru_
Content-Type: text/plain; charset="koi8-r"
Content-Transfer-Encoding: quoted-printable

    wow

--_000_36b4ab7cc0584c0487ea409534631c61EXMB02eduinnopolisru_
Content-Type: text/html; charset="koi8-r"
Content-Transfer-Encoding: quoted-printable

<html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dkoi8-r">
<style type=3D"text/css" style=3D"display:none"><!--P{margin-top:0;margin-b=
ottom:0;} --></style>
</head>
<body dir=3D"ltr" style=3D"font-size:12pt;color:#000000;background-color:#F=
FFFFF;font-family:Calibri,Arial,Helvetica,sans-serif;">
<p>    wow<br>
</p>
</body>
</html>

--_000_36b4ab7cc0584c0487ea409534631c61EXMB02eduinnopolisru_--
```

Here you can see a very difficult message for a local user

3.2 Sending email by telnet command

When sending by telnet we have to follow this command sequence: HELO (hostname) → MAIL FROM: (address) → RCPT TO: (address) → DATA: (data finishing by '.') → QUIT. Example of telnet log is shown below.

```
telnet st5.os3.su 25

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 st5.os3.su ESMTP Sendmail 8.15.2/8.15.2/Debian-3; Wed,
7 Sep 2016 20:09:48 +0300; (No UCE/UBE) logging access
from: localhost(OK)-localhost [127.0.0.1]
HELO st5.os3.su
250 st5.os3.su Hello localhost [127.0.0.1], pleased to meet you
MAIL FROM: a.tykushin@st5.os3.su
250 2.1.0 a.tykushin@st5.os3.su... Sender ok
RCPT TO: tyvision@st5.os3.su
250 2.1.5 tyvision@st5.os3.su... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: Feel it

Now we're gonna start.
.
250 2.0.0 u87H9mH2007182 Message accepted for delivery
```

```
QUIT
221 2.0.0 st5.os3.su closing connection
Connection closed by foreign host.


========================================================================
RECEIVED MESSAGE
========================================================================


From a.tykushin@st5.os3.su  Wed Sep  7 20:11:20 2016
Return-Path: <a.tykushin@st5.os3.su>
Received: from st5.os3.su (localhost [127.0.0.1])
by st5.os3.su (8.15.2/8.15.2/Debian-3) with SMTP id u87H9mH2007182
for tyvision@st5.os3.su; Wed, 7 Sep 2016 20:10:26 +0300
Date: Wed, 7 Sep 2016 20:09:48 +0300
From: a.tykushin@st5.os3.su
Message-Id: <201609071710.u87H9mH2007182@st5.os3.su>
Subject: Feel it

Now we're gonna start.
```

3.3   Postmaster mail

Make sure that messages can be delivered for postmaster@st5.os3.su
Postmaster is nothing but default alias of user root. So this mail comes to the root mailbox. Message was send by using command **sendmail postmaster@st5.os3.su** with filling fields MAIL FROM and DATA. Result of income message is shown below.

```
From tyvision Thu Sep 15 22:46:47 2016
Return-Path: <tyvision>
Received: (from tyvision@localhost)
by st5.os3.su (8.15.2/8.15.2/Submit) id u8FJklW9002712
for postmaster@st5.os3.su; Thu, 15 Sep 2016 22:46:47 +0300
Date: Thu, 15 Sep 2016 22:46:47 +0300
From: tyvision <tyvision>
Message-Id: <201609151946.u8FJklW9002712@st5.os3.su>


MAIL FROM: me@outlook.com
DATA: wowowo
```

4   Mail backup

4.1   DNS configuration for backup MTA's

```
file: st5.os3.su.zone
--------------------------------------------------------------------------------
              ADDED some additional backup emails
--------------------------------------------------------------------------------


    MX 20 mail.st2.os3.su. -- 2nd in priority points to st2 mail server (for backup)
    MX 30 mail.st3.os3.su. -- 3rd in priority points to st3 mail server (for backup)
mail.st2.os3.su.   IN  A      188.130.155.35      ; Artyom
mail.st3.os3.su.   IN  A      188.130.155.36      ; Aidar
```

4.2   MTA configuration for backup

List of files that we need to change:

/etc/mail/access this files contains configuration of access control list (email adresses, domain names, subnets)

/etc/mail/mailertable contains information hot to send mail to the final recipient

First of all, my MTA (sendmail) didn't have this files. Reconfiguration fixed it. Two records were added to **/etc/mail/sendmail.mc** file. And then **sendmailconfig** command was run.

```
FEATURE('access_db', , 'skip')dnl
FEATURE('mailertable', 'hash -o /etc/mail/mailertable')dnl
```

```
-------------------------------------------------
after sendmailconfig
-------------------------------------------------
configuration written to /etc/mail/access

127.0.0.1 OK
ClientRate:127.0.0.1 0
ClientRate: 10
ClientConn:127.0.0.1 0
ClientConn: 10
GreetPause:localhost 0        ; up to this - default records
To:st5.os3.su RELAY           ; added
To:st3.os3.su RELAY           ; added -> backup MTA for my domain
;(according to DNS records this is 2nd priority
To:st2.os3.su RELAY           ; added -> backup MTA for my domain (1st in priority)
; RELAY means: accept mail addressed to the indicated domain or received from the
; indicated domain for relaying through your SMTP server. RELAY also
; serves as an implicit OK for the other checks.
; THEORETICALLY, I can also make a white list: refuse all mail
and enable relay to 2 backup servers and myself.
-------------------------------------------------
configuration written to /etc/mail/mailertable

st5.os3.su  smtp:mail.st5.os3.su
```

4.3   Backup logs

After shutting down own MTA (command: **sudo service sendmail stop**) a couple of messages was sent from mail exchange server in @innopolis.ru.
MTA of st2.os3.su was also shutted down. In appendix A.1 are shown logs of st3.os3.su when he's got an incoming mail. In appendix A.2 are shown logs of st5.os3.su after start-up.

5   Client access and MTA internals

5.1   Choose a console mail client that is available from Ubuntu repositories

5.1.1   Where does the client store read emails?

According to the mutt guide (link) received mail is stored in **/home/user/mail/received**. But even those all emails store at **/var/mail/tyvision** (according to user name)

5.1.2   In what format?

Mutt has 4 different folder formats (link):

- mbox - plain text file

- maildir - is a directory with exactly three subdirectories "new", "cur", and "tmp". Each message is a separate file.

- MH - is a directory containing either a .mh-sequences or .xmhcache file. Messages are separate files that are numbered sequentially. MH is rarely used, most prefer the maildir format

- MMDF - variant of inbox format. each message surrounded by AAAA (fours control-A's). *Not recommended*

As a default configuration mutt uses mbox format.

5.2 Explaining queries

5.2.1 What mail queues sendmail uses?

It uses FIFO queues. List of parameters, with which we can configure queue:

CheckpointInterval=N - checkpoint queue runs after N successful deliveries

QueueFileMode=0640 - queue file mode

QueueFactor=N - slope of queue-only function

MaxQueueChildren - limit on number of concurrent queue runners

MaxRunnersPerQueue - maximum number of queue-runners per queue-grouping mith multiple queues

NiceQueueRun - priority of queue runners (nice(3))

QueueSortOrder - type of sorting in queue: by hostname/priority

MinQueueAge - minimum time in queue before retry

MaxQueueAge - maximum time in queue before rytry (if ¿ 0; only for exponental delay)

MaxQueueRunSize - how many jobs can you process in the queue

QueueDirectory - /var/spool/mqueue

Timeout.queuereturn (structure) could be in d-days, s-seconds, h-hours. Contains a couple of fields (they are just like default values for administator):

- normal
- urgent
- non-urgent
- dsn

QueueLA load average at which we just queue messages

5.2.2 What is queues purpose?

Queues are used to store messages for further transmittion of them to the recipient.

5.2.3 Location of queues on my machine

This data can be found in file **/etc/mail/databases**. According to it:

- msp queue dir is: /var/spool/mqueue-client
- queue dir is: /var/spool/mqueue

5.2.4 Interaction with queues

You can interact with queues by using mailq(see utility description later) and sendmail (e.g. to force sending). Mailq prints a summary of the mail messages queued for future delivery. You can watch queue status by typing command **/usr/bin/mailq — more**

Result will be in that form:

```
MSP Queue status...
/var/spool/mqueue-client is empty
Total requests: 0
MTA Queue status...
/var/spool/mqueue is empty
Total requests: 0
```

Also you can force sending data from queue to recipient. To do that you should type **sendmail -f**

Appendices

A   Backup mail logs

A.1   Log from backup MTA

```
----------------------------------------------
first message: st5.os3.su is down
----------------------------------------------
Sep 15 21:10:56 a-pc postfix/postqueue[18534]: inet_addr_local: configured 2 IPv4 addresses
Sep 15 21:15:57 a-pc postfix/smtpd[18559]: connect from unknown[10.90.104.9]
Sep 15 21:15:57 a-pc postfix/smtpd[18559]: 8B0D036C02E6: client=unknown[10.90.104.9]
Sep 15 21:15:57 a-pc postfix/cleanup[18563]: 8B0D036C02E6: message-id=<1473963337262.50932@innopolis.ru>
Sep 15 21:15:57 a-pc postfix/qmgr[7110]: 8B0D036C02E6: from=<a.tykushin@innopolis.ru>,
        size=2749, nrcpt=1 (queue active)
Sep 15 21:15:57 a-pc postfix/smtpd[18559]: disconnect from unknown[10.90.104.9]
        ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Sep 15 21:16:01 a-pc postfix/smtp[18564]: connect to mail.st5.os3.su[188.130.155.38]:25:
        Connection refused      -- st5.os3.su is DOWN
Sep 15 21:16:01 a-pc postfix/smtp[18564]: connect to mail.st2.os3.su[188.130.155.35]:25:
        Connection refused      -- trying to recend mail to st2 (1st in priority, but it's shutted down)
Sep 15 21:16:02 a-pc postfix/smtp[18564]: 8B0D036C02E6: to=<a.tykushin@st5.os3.su>,
        relay=none, delay=4.4, delays=0.07/0.02/4.3/0, dsn=4.4.1, status=deferred (connect to
        mail.st2.os3.su[188.130.155.35]:25: Connection refused)


----------------------------------------------
second message st5.os3.su is down
----------------------------------------------
Sep 15 21:17:22 a-pc postfix/smtpd[18559]: connect from unknown[10.90.104.83]
Sep 15 21:17:23 a-pc postfix/smtpd[18559]: 5CFBA36C0551: client=unknown[10.90.104.83]
Sep 15 21:17:23 a-pc postfix/cleanup[18563]: 5CFBA36C0551:
        message-id=<36b4ab7cc0584c0487ea409534631c61@EXMB02.edu.innopolis.ru>
Sep 15 21:17:23 a-pc postfix/qmgr[7110]: 5CFBA36C0551: from=<a.tykushin@innopolis.ru>,
        size=2130, nrcpt=1 (queue active)
Sep 15 21:17:23 a-pc postfix/smtpd[18559]: disconnect from unknown[10.90.104.83]
        ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Sep 15 21:17:26 a-pc postfix/smtp[18564]: connect to mail.st2.os3.su[188.130.155.35]:25:
        Connection refused
Sep 15 21:17:26 a-pc postfix/smtp[18564]: 5CFBA36C0551: to=<a.tykushin@st5.os3.su>,
        relay=none, delay=3, delays=0.5/0/2.5/0, dsn=4.4.1, status=deferred (connect to
        mail.st2.os3.su[188.130.155.35]:25: Connection refused)


----------------------------------------------
trying to send to a.tykushin@st5.os3.su:
----------------------------------------------
Sep 15 21:17:46 a-pc postfix/postqueue[18573]: name_mask: ipv4
Sep 15 21:17:46 a-pc postfix/postqueue[18573]: inet_addr_local: configured 2 IPv4 addresses
Sep 15 21:17:46 a-pc postfix/qmgr[7110]: 8B0D036C02E6: from=<a.tykushin@innopolis.ru>,
        size=2749, nrcpt=1 (queue active)
Sep 15 21:17:46 a-pc postfix/qmgr[7110]: 5CFBA36C0551: from=<a.tykushin@innopolis.ru>,
        size=2130, nrcpt=1 (queue active)
Sep 15 21:17:49 a-pc postfix/smtp[18564]: 8B0D036C02E6: to=<a.tykushin@st5.os3.su>,
        relay=st5.os3.su[188.130.155.38]:25, delay=111, delays=109/0/1.4/0.69, dsn=2.0.0,
        status=sent (250 2.0.0 u8FIHVf2001667 Message accepted for delivery)
        -- first message is sent
Sep 15 21:17:49 a-pc postfix/qmgr[7110]: 8B0D036C02E6: removed      -- removed from the queue
Sep 15 21:17:50 a-pc postfix/smtp[18574]: connect to mail.st2.os3.su[188.130.155.35]:25:
        Connection refused
Sep 15 21:17:50 a-pc postfix/smtp[18574]: 5CFBA36C0551: to=<a.tykushin@st5.os3.su>,
        relay=none, delay=28, delays=24/0/4/0, dsn=4.4.1, status=deferred (connect to
        mail.st2.os3.su[188.130.155.35]:25: Connection refused)
```

```
          -- failure on sending second message


--------------------------------------------------
forcing queue: when my MTA was up
--------------------------------------------------
Sep 15 21:20:33 a-pc postfix/postqueue[18580]: name_mask: ipv4
Sep 15 21:20:33 a-pc postfix/postqueue[18580]: inet_addr_local: configured 2 IPv4 addresses
Sep 15 21:20:33 a-pc postfix/qmgr[7110]: 5CFBA36C0551: from=<a.tykushin@innopolis.ru>,
       size=2130, nrcpt=1 (queue active)
Sep 15 21:20:36 a-pc postfix/smtp[18582]: 5CFBA36C0551: to=<a.tykushin@st5.os3.su>,
       relay=st5.os3.su[188.130.155.38]:25, delay=194, delays=190/0/3/0.4, dsn=2.0.0,
       status=sent (250 2.0.0 u8FIKJds001719 Message accepted for delivery)
       -- second message is sent
Sep 15 21:20:36 a-pc postfix/qmgr[7110]: 5CFBA36C0551: removed      -- removed from queue
Sep 15 21:20:44 a-pc postfix/anvil[18561]: statistics:
       max connection rate 1/60s for (smtp:10.90.104.9) at Sep 15 21:15:57
Sep 15 21:20:44 a-pc postfix/anvil[18561]: statistics:
       max connection count 1 for (smtp:10.90.104.9) at Sep 15 21:15:57
Sep 15 21:20:44 a-pc postfix/anvil[18561]: statistics: max cache size 1 at Sep 15 21:15:57
```

A.2   Log from own MTA

```
--------------------------------------------------
starting up own MTA
--------------------------------------------------
Sep 15 21:17:22 st5 sm-mta[1652]: starting daemon (8.15.2): SMTP+queueing@00:10:00
       -- start SENDMAIL
Sep 15 21:17:33 st5 sm-mta[1667]: u8FIHVf2001667: from=<a.tykushin@innopolis.ru>,
       size=2676, class=0, nrcpts=1, msgid=<1473963337262.50932@innopolis.ru>,
       proto=ESMTP, daemon=MTA-v4, relay=mail.st3.os3.su [188.130.155.36]
Sep 15 21:17:33 st5 sm-mta[1668]: u8FIHVf2001667: to=tyvision@st5.os3.su, delay=00:00:01,
       xdelay=00:00:00, mailer=local, pri=32865, dsn=2.0.0, stat=Sent
       -- got 1st message
Sep 15 21:20:21 st5 sm-mta[1719]: u8FIKJds001719: from=<a.tykushin@innopolis.ru>,
       size=2078, class=0, nrcpts=1,
       msgid=<36b4ab7cc0584c0487ea409534631c61@EXMB02.edu.innopolis.ru>, proto=ESMTP,
       daemon=MTA-v4, relay=mail.st3.os3.su [188.130.155.36]
Sep 15 21:20:21 st5 sm-mta[1721]: u8FIKJds001719: to=tyvision@st5.os3.su,
       delay=00:00:00, xdelay=00:00:00, mailer=local, pri=32269, dsn=2.0.0, stat=Sent
       -- got 2nd message (after force queue from st3.os3.su)
```