

Администрирование сетевых подсистем

Настройка SMTP-аутентификации и SMTP over TLS

Заур Мустафаев

05 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цели работы

Получение навыков настройки SMTP-аутентификации и защищённого SMTP over TLS на базе Postfix и Dovecot.

Выполнение работы

Добавление протокола LMTP в Dovecot

```
dovecot.conf [----] 26 L:[ 1+24 25/103] *(1182/4322b) 0010 0x00A
## Dovecot configuration file

# If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration

# "doveconf -n" command gives a clean output of the changed settings. Use it
# instead of copy&pasting files when posting to the Dovecot mailing list.

# '#' character and everything after it is treated as comments. Extra spaces
# and tabs are ignored. If you want to use either of these explicitly, put the
# value inside quotes, eg.: key = "# char and trailing whitespace "

# Most (but not all) settings can be overridden by different protocols and/or
# source/destination IPs by placing the settings inside sections, for example:
# protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }

# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

# Protocols we want to be serving.

protocols = imap pop3 lmtp

# A comma separated list of IPs or hosts where to listen in for connections..
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
```

Настройка сервиса LMTP

```
10-master.conf [----] 14 L:[ 49+ 8 57/130] *(1424/3511b) 0010 0x00A
inet_listener submission {
    #port = 587
}
inet_listener submissions {
    #port = 465
}
}

service lmtp {
    unix_listener /var/spool/postfix/private/dovecot-lmtp {
        group = postfix
        user = postfix
        mode = 0600
    }
}
```

Рис. 2: Настройка сервиса LMTP

Настройка формата логина

```
10-auth.conf      [----] 26 L:[ 44+ 8 52/129] *(2503/5248b) 0010 0x00A
# that '#' and '/' characters are translated to '@'.
#auth_username_translation =

# Username formatting before it's looked up from databases. You can use
# the standard variables here, eg. %Lu would lowercase the username, %n would
# drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
# "-AT-". This translation is done after auth_username_translation changes.

auth_username_format = %Ln

# If you want to allow master users to log in by specifying the master
# username within the normal username string (ie. not using SASL mechanism's
# support for it), you can specify the separator character here. The format
# is then <username><separator><master username>. UW-IMAP uses "*" as the
# separator, so that could be a good choice.
#auth_master_user_separator =

# Username to use for users logging in with ANONYMOUS SASL mechanism
#auth_anonymous_username = anonymous

# Maximum number of dovecot-auth worker processes. They're used to execute
# blocking passwd and userdb queries (eg. MySQL and PAM). They're
# automatically created and destroyed as needed.
#auth_worker_max_count = 30

# Host name to use in GSSAPI principal names. The default is to use the
# name returned by gethostname(). Use "$ALL" (with quotes) to allow all keytab
# entries.
#auth_gssapi_hostname =
```

```
[zmustafaev@client.zmustafaev.net ~]$ echo . | mail -s "LMTP test" zmustafaev@zmu  
stafaev.net  
[zmustafaev@client.zmustafaev.net ~]$ █
```

Рис. 4: Отправка письма


```
Nov  4 09:00:47 server postfix/smtpd[15708]: connect from client.zmustafaev.net[192.168.1.30]
Nov  4 09:00:47 server postfix/smtpd[15708]: C59A120F624E: client=client.zmustafaev.net[192.168.1.30]
Nov  4 09:00:47 server postfix/cleanup[15712]: C59A120F624E: message-id=<20251104090047.B8F711FB4A@client.zmustafaev.net>
Nov  4 09:00:47 server postfix/smtpd[15708]: disconnect from client.zmustafaev.net[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Nov  4 09:00:47 server postfix/qmgr[15525]: C59A120F624E: from=<zmustafaev@client.zmustafaev.net>, size=561, nrcpt=1 (queue active)
Nov  4 09:00:47 server postfix/local[15713]: C59A120F624E: passing <zmustafaev@zmustafaev.net> to transport=lmtp
Nov  4 09:00:47 server dovecot[15562]: lmtp(15715): Connect from local
Nov  4 09:00:47 server dovecot[15562]: lmtp(zmustafaev)<15715><d8tgMb/ACWljPQAAzb6wxg>: msgid=<20251104090047.B8F711FB4A@client.zmustafaev.net>: saved mail to INBOX
Nov  4 09:00:47 server postfix/lmtp[15714]: C59A120F624E: to=<zmustafaev@zmustafaev.net>, relay=server.zmustafaev.net[private/dovecot-lmtp], delay=0.04, delays=0.01/0/0.01/0.01, dsn=2.0.0, status=sent (250 2.0.0 <zmustafaev@zmustafaev.net> d8tgMb/ACWljPQAAzb6wxg Saved)
Nov  4 09:00:47 server dovecot[15562]: lmtp(15715): Disconnect from local: Logged out (state=READY)
Nov  4 09:00:47 server postfix/qmgr[15525]: C59A120F624E: removed
```

Рис. 5: Журналы LMTP

```
[zmustafaev@server.zmustafaev.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.24.  Type '?' for help
/home/zmustafaev/Maildir: 2 messages 1 new
      1 zmustafaev          2025-10-29 15:09    18/668    "test1
►N    2 zmustafaev@client.zm 2025-11-04 09:00    21/855    "LMTP test
&
[-- Message 2 -- 21 lines, 855 bytes --]:
Date: Tue, 04 Nov 2025 09:00:47 +0000
To: zmustafaev@zmustafaev.net
Subject: LMTP test
Message-Id: <20251104090047.B8F711FB4A@client.zmustafaev.net>
From: zmustafaev@client.zmustafaev.net

.

& q
Held 2 messages in /home/zmustafaev/Maildir
[zmustafaev@server.zmustafaev.net ~]$
```

```
10-master.conf [----] 0 L:[ 79+18 97/115] *(2180/2636b) 0125 0x07

service submission {
    # Max. number of SMTP Submission processes (connections)
    #process_limit = 1024
}

service auth {
    unix_listener auth-userdb {
        mode = 0600
        user = dovecot
    }

    unix_listener /var/spool/postfix/private/auth {
        group = postfix
        user = postfix
        mode = 0660
    }
}
```

Рис. 7: Сервис auth в Dovecot

```
[root@server.zmustafaev.net ~]#  
[root@server.zmustafaev.net ~]# postconf -e 'smtpd_sasl_type = dovecot'  
[root@server.zmustafaev.net ~]# postconf -e 'smtpd_sasl_path = private/auth'  
[root@server.zmustafaev.net ~]#  
[root@server.zmustafaev.net ~]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain  
, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, per  
mit'  
[root@server.zmustafaev.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'  
[root@server.zmustafaev.net ~]#
```

Рис. 8: Команды postconf

Изменения master.cf

```
master.cf      [-M--] 1 L:[ 1+ 0 1/148] *(1 /7217b) 0010 0x00A
#
# Postfix master process configuration file. For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
# =====
# service type private unpriv chroot wakeup maxproc command + args
#          (yes)   (yes)   (no)   (never) (100)
# =====
smtp      inet  n       -       n       -       -       smtpd
#smtp     inet  n       -       n       -       1       postscreen
#smtpd    pass  -       -       n       -       -       smtpd
#dnsblog  unix  -       -       n       -       0       dnsblog
#tlsproxy unix  -       -       n       -       0       tlsproxy
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n - n - - smtpd
#submission inet n - n - - smtpd
#  -o syslog_name=postfix/submission
#  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_tls_auth_only=yes
#  -o local_header_rewrite_clients=static:all
#  -o smtpd_reject_unlisted_recipient=no
#
# Instead of specifying complex smtpd_<xxx>_restrictions here,
# specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
# here, and specify mua_<xxx>_restrictions in main.cf (where
# "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
```

Проверка SMTP AUTH через telnet

```
[root@client.zmustafaev.net ~]# printf 'zmustafaev\x00zmustafaev\x00123456' | base64
em11c3RhZmFldgB6bXVzdGFmYWV2ADEyMzQ1Ng==
[root@client.zmustafaev.net ~]#
[root@client.zmustafaev.net ~]# telnet server.zmustafaev.net 25
Trying 192.168.1.1...
Connected to server.zmustafaev.net.
Escape character is '^]'.
220 server.zmustafaev.net ESMTP Postfix
EHLO test
250-server.zmustafaev.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN em11c3RhZmFldgB6bXVzdGFmYWV2ADEyMzQ1Ng==
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
Connection closed by foreign host.
[root@client.zmustafaev.net ~]#
```

Копирование сертификата Dovecot

```
[root@server.zmustafaev.net ~]#  
[root@server.zmustafaev.net ~]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs/  
[root@server.zmustafaev.net ~]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private/  
[root@server.zmustafaev.net ~]# postconf -e 'smtpd_tls_cert_file = /etc/pki/tls/certs/dovecot.pem'  
[root@server.zmustafaev.net ~]# postconf -e 'smtpd_tls_key_file = /etc/pki/tls/private/dovecot.pem'  
[root@server.zmustafaev.net ~]# postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtp  
d_scache'  
[root@server.zmustafaev.net ~]# postconf -e 'smtpd_tls_security_level = may'  
[root@server.zmustafaev.net ~]# postconf -e 'smtp_tls_security_level = may'  
[root@server.zmustafaev.net ~]#
```

Рис. 11: TLS — копирование сертификатов

master.cf — порт 587 (submission)

```
master.cf      [----]  0 L:  5+16  21/148] *(1113/7215b) 0032 0x020
#
# Do not forget to execute "postfix reload" after editing this file.
#
# =====
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# =====
smtp           inet  n       -       n       -       -       smtpd
#smtp          inet  n       -       n       -       1       postscreen
#smtpd         pass  -       -       n       -       -       smtpd
#dnsblog       unix  -       -       n       -       0       dnsblog
#tlsproxy      unix  -       -       n       -       0       tlsproxy
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n - n - - smtpd
submission    inet  n       -       n       -       -       smtpd
#
# -o syslog_name=postfix/submission
# -o smtpd_tls_security_level=encrypt
# -o smtpd_sasl_auth_enable=yes
# -o smtpd_tls_auth_only=yes
#
# -o local_header_rewrite_clients=static:all
#
# -o smtpd_reject_unlisted_recipient=no
#
#   Instead of specifying complex smtpd_<xxx>_restrictions here,
#   specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
#   here, and specify mua_<xxx>_restrictions in main.cf (where
#   "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
#
# -o smtpd_client_restrictions=
#
# -o smtpd_helo_restrictions=
#
# -o smtpd_sender_restrictions=
#
# -o smtpd_relay_restrictions=
```


Проверка подключения по TLS (openssl)

```
00c0 - 66 bf 04 3f c5 2e 0b c7-bd 53 f6 6d 68 e7 5a 7f  f..?.....S.mh.Z.

Start Time: 1762248032
Timeout   : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0

---
read R BLOCK
EHLO test
250-server.zmustafaev.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN em11c3RhZmFlZdB6bXVzdGFmYWV2ADEyMzQ1Ng==
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
closed
[root@client.zmustafaev.net ~]#
```

SMTP-клиент Evolution — настройка отправки почты

Account Editor ✕

Identity

Receiving Email

Receiving Options

Sending Email

Defaults

Composing Messages

Security

Server Type: **SMTP**

Description: For delivering mail by connecting to a remote mailhub using SMTP.

Configuration

Server: Port: ▼

☒ Server requires authentication

Security

Encryption method: ▼

Authentication

Type: ▼

Username:

Send Options

☐ Re-encode message before send

Получение письма через TLS + LMTP

The screenshot displays an email client interface. At the top, there's a toolbar with icons for Send/Receive, Reply, Group Reply, and Forward. Below this is a navigation pane on the left with folders like Inbox (1 unread, 3 total), Drafts, Junk, Outbox, Sent, Templates, and Trash. A section titled 'News and Blogs' is also visible. The main pane shows a list of messages in the inbox. The selected message is from zmustafaev@client.zmustafaev.net with subject 'LMTP test' and received today at 09:00. Below the message list, the details of the selected email are shown, including the sender, recipient, subject, and date.

Inbox (1 unread, 3 total)

Show: All Messages Search: Subject or Ad... in Current Folder

From	Subject	Date	To Do
zmustafaev <zmustafa...	test1	Wed 15:09	Today
zmustafaev@client.zm...	LMTP test	Today 09:00	Tomori
zmustafaev <zmust...	test3	Today 09:22	11/06,

News and Blogs

▼ zmustafaev@zmu... ↔

Inbox (1)

Junk

Mail

Contacts

Calendar

Tasks

Memos

Reply Group Reply Forward

From: zmustafaev@client.zmustafaev.net
To: zmustafaev@zmustafaev.net
Subject: LMTP test
Date: Tue, 04 Nov 2025 09:00:47 +0000

```
Nov  4 09:22:16 server postfix/smtpd[18539]: connect from client.zmustafaev.net[192.168.1.30]
Nov  4 09:22:16 server postfix/tlsmgr[18541]: warning: btree:/var/lib/postfix/smtpd_scache is unavailable.
unsupported dictionary type: btree
Nov  4 09:22:20 server postfix/smtpd[18539]: 737ED20F5FD0: client=client.zmustafaev.net[192.168.1.30], sasl
_method=PLAIN, sasl_username=zmustafaev
Nov  4 09:22:20 server postfix/cleanup[18963]: 737ED20F5FD0: message-id=<5b50ea18b8a10b838287920765db7df5c8
a90268.camel@zmustafaev.net>
Nov  4 09:22:20 server postfix/qmgr[18374]: 737ED20F5FD0: from=<zmustafaev@zmustafaev.net>, size=561, nrcpt
=1 (queue active)
Nov  4 09:22:20 server postfix/smtpd[18539]: disconnect from client.zmustafaev.net[192.168.1.30] ehlo=2 sta
rttls=1 auth=1 mail=1 rcpt=1 data=1 quit=1 commands=8
Nov  4 09:22:20 server postfix/local[18964]: 737ED20F5FD0: passing <zmustafaev@zmustafaev.net> to transport
=lmp
Nov  4 09:22:20 server dovecot[17254]: lmp(18966): Connect from local
Nov  4 09:22:20 server dovecot[17254]: lmp(zmustafaev)<18966><PnrthMzFCWkWSgAAzb6wxg>: msgid=<5b50ea18b8a1
0b838287920765db7df5c8a90268.camel@zmustafaev.net>: saved mail to INBOX
Nov  4 09:22:20 server postfix/lmp[18965]: 737ED20F5FD0: to=<zmustafaev@zmustafaev.net>, relay=server.zmus
tafaev.net[private/dovecot-lmp], delay=0.02, delays=0.01/0/0.01/0, dsn=2.0.0, status=sent (250 2.0.0 <zmus
tafaev@zmustafaev.net> PnrthMzFCWkWSgAAzb6wxg Saved)
Nov  4 09:22:20 server dovecot[17254]: lmp(18966): Disconnect from local: Logged out (state=READY)
Nov  4 09:22:20 server postfix/qmgr[18374]: 737ED20F5FD0: removed
```

Рис. 16: Логи TLS Доставки

Вывод

В результате работы:

- Настроено взаимодействие **Postfix** ↔ **Dovecot** через **LMTP**
- Реализована **SMTP-аутентификация** (**SASL**, **unix-socket**)
- Настроен **SMTP over TLS** (**587** / **STARTTLS**)
- Доставку писем проверили через **telnet**, **openssl** и почтовый клиент
- Конфигурация автоматизирована через **provisioning-скрипты Vagrant**