

Администрирование системных подсистем

Настройка SMTP, LMTP, SASL и TLS на Postfix + Dovecot

Сейдалиев Тагьетдин Ровшенович

30 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получение практических навыков настройки SMTP-сервера Postfix и Dovecot: LMTP, аутентификация SASL, TLS-шифрование.

Настройка LMTP в Dovecot

Добавляем LMTP в конфигурацию Dovecot.

```
1 ## Dovecot configuration file
2
3 # If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration
4
5 # "doveconf -n" command gives a clean output of the changed settings. Use it
6 # instead of copy&pasting files when posting to the Dovecot mailing list.
7
8 # '#' character and everything after it is treated as comments. Extra spaces
9 # and tabs are ignored. If you want to use either of these explicitly, put the
10 # value inside quotes, eg.: key = "# char and trailing whitespace "
11
12 # Most (but not all) settings can be overridden by different protocols and/or
13 # source/destination IPs by placing the settings inside sections, for example:
14 # protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }
15
16 # Default values are shown for each setting, it's not required to uncomment
17 # those. These are exceptions to this though: No sections (e.g. namespace {})
18 # or plugin settings are added by default, they're listed only as examples.
19 # Paths are also just examples with the real defaults being based on configure
20 # options. The paths listed here are for configure --prefix=/usr
21 # --sysconfdir=/etc --localstatedir=/var
22
23 # Protocols we want to be serving.
24
```

Настройка LMTP-сервиса

Определяем сокет LMTP для взаимодействия Postfix и Dovecot.



```
Open ▼ + 10-master.conf /etc/dovecot/conf.d
44 #ssl = yes
45 }
46 }
47
48 service submission-login {
49   inet_listener submission {
50     #port = 587
51   }
52   inet_listener submissions {
53     #port = 465
54   }
55 }
56
57 service lmtp {
58   unix_listener /var/spool/postfix/private/dovecot-lmtp {
59     group = postfix
60     user = postfix
61     mode = 0600
62   }
63
64
```

Задаём формат логина без доменной части.

```
46
47 # Username formatting before it's looked up from databases. You can use
48 # the standard variables here, eg. %Lu would lowercase the username, %n would
49 # drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
50 # "-AT-". This translation is done after auth_username_translation changes.
51
52 auth_username_format = %Ln|
```

Рис. 3: auth_username_format

Подтверждение доставки письма в INBOX через LMTP.

```
Nov 30 11:11:18 server postfix/smtpd[24038]: connect from client.trseidaliev.net[192.168.1.30]
Nov 30 11:11:18 server postfix/smtpd[24038]: 19F35239C170: client=client.trseidaliev.net[192.168.1.30]
Nov 30 11:11:18 server postfix/cleanup[24042]: 19F35239C170: message-id=<20251130081116.948362368984@client.trseidaliev.net>
Nov 30 11:11:18 server postfix/smtpd[24038]: disconnect from client.trseidaliev.net[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Nov 30 11:11:18 server postfix/qmgr[23929]: 19F35239C170: from=<trseidaliev@client.trseidaliev.net>, size=576, nrcpt=1 (queue active)
Nov 30 11:11:18 server postfix/local[24043]: 19F35239C170: passing <trseidaliev@trseidaliev.net> to transport=lmtp
Nov 30 11:11:18 server dovecot[23976]: lmtp(24045): Connect from local
Nov 30 11:11:18 server dovecot[23976]: lmtp(trseidaliev)<24045><XAI2Byb8K2ntXQAAe9wJyQ>: msgid=<20251130081116.948362368984@client.trseidaliev.net>; saved mail to INBOX
Nov 30 11:11:18 server postfix/lmtp[24044]: 19F35239C170: to=<trseidaliev@trseidaliev.net>, relay=server.trseidaliev.net[private/dovecot-lmtp], delay=0.03, delays=0.01/0/0.01/0.01, dsn=2.0.0, status=sent (250 2.0.0 <trseidaliev@trseidaliev.net> XAI2Byb8K2ntXQAAe9wJyQ Saved)
Nov 30 11:11:18 server dovecot[23976]: lmtp(24045): Disconnect from local: Logged out (state=READY)
Nov 30 11:11:18 server postfix/qmgr[23929]: 19F35239C170: removed
```

Рис. 4: Логи LMTP

Письмо отображается в пользовательском почтовом ящике.

```
[trseidaliev@server.trseidaliev.net server]$  
[trseidaliev@server.trseidaliev.net server]$ MAIL=~/.Maildir/ mail  
s-nail version v14.9.24. Type '?' for help  
/home/trseidaliev/Maildir: 2 messages 1 new  
      1 trseidaliev      2025-11-30 10:46      18/685      "test1  
▶N  2 trseidaliev@client.t 2025-11-30 11:11      21/880      "LMTP TEST  
&  
[-- Message  2 -- 21 lines, 880 bytes --]:  
Date: Sun, 30 Nov 2025 08:11:16 +0000  
To: trseidaliev@trseidaliev.net  
Subject: LMTP TEST  
Message-Id: <20251130081116.948362368984@client.trseidaliev.net>  
From: trseidaliev@client.trseidaliev.net  
  
.  
  
& q  
Held 2 messages in /home/trseidaliev/Maildir  
[trseidaliev@server.trseidaliev.net server]$
```

Настройка SMTP-аутентификации

Настраивается сокет для SASL-аутентификации Postfix.

```
83
84 service auth {
85     unix_listener auth-userdb {
86         mode = 0600
87         user = dovecot
88     }
89
90     unix_listener /var/spool/postfix/private/auth
91         group = postfix
92         user = postfix
93         mode = 0660
94
95
96     # Auth process is run as this user.
97     #user = $default_internal_user
98 }
```

Рис. 6: auth service

Postfix использует Dovecot как механизм SASL.

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

Рис. 7: postconf sasl

Настраиваются правила защиты от open relay.

```
1 #
2 # Postfix master process configuration file. For details on the format
3 # of the file, see the master(5) manual page (command: "man 5 master" or
4 # on-line: http://www.postfix.org/master.5.html).
5 #
6 # Do not forget to execute "postfix reload" after editing this file.
7 #
8 # -----
9 # service type  private unpriv  chroot  wakeup  maxproc command + args
10 #              (yes)   (yes)   (no)    (never) (100)
11 # -----
12 smtp      inet  n       -       n       -       -       smtpd
13 #smtp      inet  n       -       n       -       1       postscreen
14 #smtpd     pass  -       -       n       -       -       smtpd
15 #dnsblog   unix  -       -       n       -       0       dnsblog
16 #tlsproxy  unix  -       -       n       -       0       tlsproxy
17 # Choose one: enable submission for loopback clients only, or for any client.
18 #127.0.0.1:submission inet n - n - - smtpd
19 #submission inet n - n - - smtpd
20 # -o syslog_name=postfix/submission
21 # -o smtpd_tls_security_level=encrypt
22 -o smtpd_sasl_auth_enable=yes
23 # -o smtpd_tls_auth_only=yes
24 # -o local_header_rewrite_clients=static:all
25 # -o smtpd_reject_unlisted_recipient=no
26 #   Instead of specifying complex smtpd_<xxx>_restrictions here,
27 #   specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
28 #   here, and specify mua_<xxx>_restrictions in main.cf (where
29 #   "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
30 # -o smtpd_client_restrictions=
31 # -o smtpd_helo_restrictions=
32 # -o smtpd_sender_restrictions=
33 # -o smtpd_relay_restrictions=
```

Проверка аутентификации

Пользователь успешно проходит SMTP AUTH.

```
[root@client.trseidaliev.net ~]# telnet server.trseidaliev.net 25
Trying 192.168.1.1...
Connected to server.trseidaliev.net.
Escape character is '^]'.
220 server.trseidaliev.net ESMTP Postfix
EHLO test
250-server.trseidaliev.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 dHJzZWlkYWxpZXYAdHJzZWlkYWxpZXYAMTIzNDU2
235 2.7.0 Authentication successful
quit
```

Настройка SMTP over TLS

Postfix использует сертификаты Dovecot для TLS.

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

Рис. 10: TLS настройка

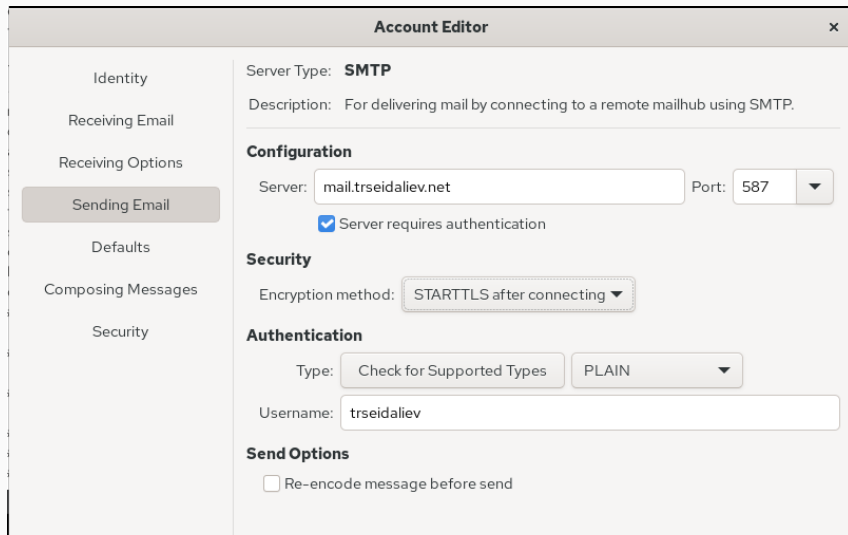
Создаётся защищённый SMTP-сервис с обязательным шифрованием.

```
1 #
2 # Postfix master process configuration file. For details on the format
3 # of the file, see the master(5) manual page (command: "man 5 master" or
4 # on-line: http://www.postfix.org/master.5.html).
5 #
6 # Do not forget to execute "postfix reload" after editing this file.
7 #
8 # -----
9 # service type private unpriv chroot wakeup maxproc command + args
10 # (yes) (yes) (no) (never) (100)
11 # -----
12 smtp inet n - n - - smtpd
13 #smtp inet n - n - 1 postscreen
14 #smtpd pass - - n - - smtpd
15 #dnsblog unix - - n - 0 dnsblog
16 #tlsproxy unix - - n - 0 tlsproxy
17 # Choose one: enable submission for loopback clients only, or for any client.
18 #127.0.0.1:submission inet n - n - - smtpd
19 submission inet n - n - - smtpd
20 # -o syslog_name=postfix/submission
21 # -o smtpd_tls_security_level=encrypt
22 # -o smtpd_sasl_auth_enable=yes
23 # -o smtpd_tls_auth_only=yes
24 # -o local_header_rewrite_clients=static:all
25 # -o smtpd_reject_unlisted_recipient=no
26 # Instead of specifying complex smtpd_<xxx>_restrictions here,
27 # specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
28 # here, and specify mua_<xxx>_restrictions in main.cf (where
29 # "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
30 # -o smtpd_client_restrictions=
31 # -o smtpd_helo_restrictions=
32 # -o smtpd_sender_restrictions=
```

Проверяется установление TLS-сессии и успешный AUTH.

```
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
EGLO test
500 5.5.2 Error: command not recognized
EHLO test
250-server.trseidaliev.net
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN dHJzZWlkYWxpZXYAdHJzZWlkYWxpZXYAMTIzNDU2
235 2.7.0 Authentication successful
quit
```

Почтовый клиент успешно использует порт 587 и STARTTLS.



The screenshot shows the 'Account Editor' window in the Evolution email client. The left sidebar contains a list of configuration categories: Identity, Receiving Email, Receiving Options, Sending Email (which is highlighted), Defaults, Composing Messages, and Security. The main panel is titled 'Account Editor' and displays the configuration for an SMTP account.

Server Type: SMTP

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

Configuration

Server: mail.trseidaliev.net Port: 587 ▼

☒ Server requires authentication

Security

Encryption method: STARTTLS after connecting ▼

Authentication

Type: Check for Supported Types PLAIN ▼

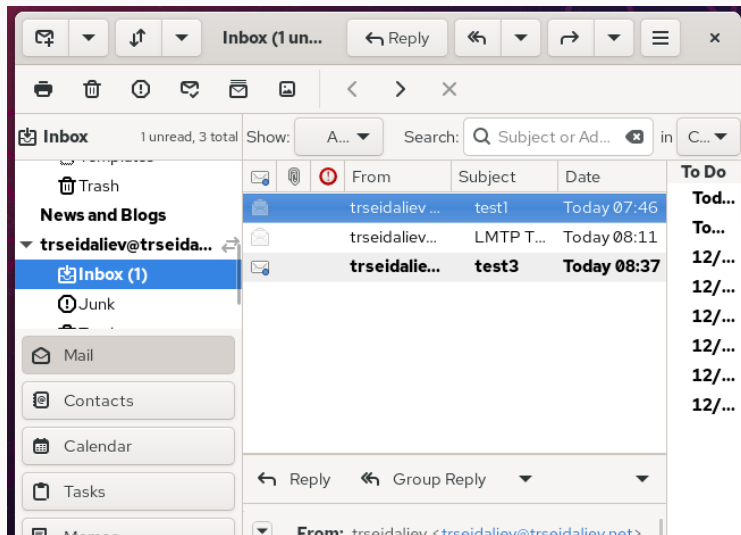
Username: trseidaliev

Send Options

☐ Re-encode message before send

Проверка доставки писем

Письма успешно доставляются через защищённый SMTP.



Журнал фиксирует успешную обработку и доставку писем.

```
Nov 30 11:37:23 server postfix/smtpd[27694]: connect from client.trseidaliev.net[192.168.1.30]
Nov 30 11:37:23 server postfix/tlsmgr[27696]: warning: btree:/var/lib/postfix/smtpd_scache is unavailable. unsupported
dictionary type: btree
Nov 30 11:37:28 server postfix/smtpd[27694]: 0BD2523AD265: client=client.trseidaliev.net[192.168.1.30], sasl_method=PL
AIN, sasl_username=trseidaliev
Nov 30 11:37:28 server postfix/cleanup[27926]: 0BD2523AD265: message-id=<c1450906964e3baa8d5dbc1785f9972d067c20cd.came
l@trseidaliev.net>
Nov 30 11:37:28 server postfix/qmgr[27581]: 0BD2523AD265: from=<trseidaliev@trseidaliev.net>, size=572, nrcpt=1 (queue
active)
Nov 30 11:37:28 server postfix/smtpd[27694]: disconnect from client.trseidaliev.net[192.168.1.30] ehlo=2 starttls=1 au
th=1 mail=1 rcpt=1 data=1 quit=1 commands=8
Nov 30 11:37:28 server postfix/local[27927]: 0BD2523AD265: passing <trseidaliev@trseidaliev.net> to transport=lmt
Nov 30 11:37:28 server dovecot[26635]: lmt(27929): Connect from local
Nov 30 11:37:28 server dovecot[26635]: lmt(trseidaliev)<27929><7WmsA0gCLGkZbQAAe9wJyQ>: msgid=<c1450906964e3baa8d5dbc
1785f9972d067c20cd.camel@trseidaliev.net>: saved mail to INBOX
Nov 30 11:37:28 server dovecot[26635]: lmt(27929): Disconnect from local: Logged out (state=READY)
Nov 30 11:37:28 server postfix/lmt[27928]: 0BD2523AD265: to=<trseidaliev@trseidaliev.net>, relay=server.trseidaliev.n
et[private/dovecot-lmt], delay=0.02, delays=0.01/0/0.01/0, dsn=2.0.0, status=sent (250 2.0.0 <trseidaliev@trseidaliev
.net> 7WmsA0gCLGkZbQAAe9wJyQ Saved)
Nov 30 11:37:28 server postfix/qmgr[27581]: 0BD2523AD265: removed
```

Рис. 15: maillog

Заключение

В ходе выполнения работы:

- настроен SMTP-сервер Postfix с поддержкой аутентификации пользователей через Dovecot;
- реализована передача почты посредством LMTP-сервиса Dovecot;
- включена и проверена работа TLS-шифрования для SMTP (порт 587, STARTTLS);
- выполнена настройка firewall для служб smtp и smtp-submission;
- протестирована SMTP-аутентификация как через telnet/openssl, так и через почтовый клиент Evolution;
- обновлены конфигурации Postfix и Dovecot в каталоге provisioning для автоматизации развёртывания.