

Администрирование сетевых подсистем

Расширенные настройки SMTP-сервера (Лабораторная работа №10)

Суннатилло Махмудов

20 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Приобретение практических навыков по конфигурированию SMTP-сервера с настройкой аутентификации и шифрования.

1. Настроить доставку почты через **LMTP** между Postfix и Dovecot.
2. Реализовать **SMTP-аутентификацию** с использованием SASL.
3. Настроить **SMTP over TLS** для защищённой передачи данных.
4. Проверить работу с помощью инструментов **telnet**, **openssl**, **Evolution**.
5. Автоматизировать конфигурацию с использованием Vagrant.

Теоретическая часть

- **Postfix** — MTA, выполняет приём и маршрутизацию сообщений.
- **Dovecot** — MDA, обеспечивает хранение и доступ к почтовым ящикам.
- **LMTP** — протокол локальной передачи между Postfix и Dovecot.
- **SASL** — механизм аутентификации в SMTP.
- **TLS/SSL** — обеспечивает шифрование при передаче почты.

Протокол	Назначение	Порт
SMTP	Передача писем между серверами	25
IMAP	Чтение почты на сервере	143
POP3	Получение писем на клиент	110
Submission (STARTTLS)	Безопасная отправка писем	587

Настройка LMTP в Dovecot

```
dovecot.conf      [----] 26 L:[ 8+17 25/104] *(1182/4323b) 0010 0x00A
# '#' 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,
# edit conf.d/master.conf.
#listen = *, ::

# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Name of this instance. In multi-instance setup doveadm and other commands
```

```
10-master.conf  [----] 11 L:[ 45+16  61/129] *(1533/3511b) 0048 0x030
}
}

service submission-login {
    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: Определение unix-сокета для LMTP

Проверка доставки письма

```
Oct 13 12:40:58 server postfix/smtpd[14717]: connect from client.snahmudov.net[192.168.1.30]
Oct 13 12:40:58 server postfix/smtpd[14717]: 5793E607700A: client=client.snahmudov.net[192.168.1.30]
Oct 13 12:40:58 server postfix/cleanup[14721]: 5793E607700A: message-id=<20251013124058.483F6273D0@client.snahmudov.net>
Oct 13 12:40:58 server postfix/smtpd[14717]: disconnect from client.snahmudov.net[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Oct 13 12:40:58 server postfix/qmgr[14463]: 5793E607700A: from=<snahmudov@client.snahmudov.net>, size=550, nrcpt=1 (queue active)
Oct 13 12:40:58 server postfix/local[14722]: 5793E607700A: passing <snahmudov@snahmudov.net> to transport=lmtp
Oct 13 12:40:58 server dovecot[14628]: lmtp(14724): Connect from local
Oct 13 12:40:58 server dovecot[14628]: lmtp(snahmudov)<14724><s3F/Flrz7GtEOQAA@WRAUQ>: msgid=<20251013124058.483F6273D0@client.snahmudov.net>: saved mail to INBOX
Oct 13 12:40:58 server dovecot[14628]: lmtp(14724): Disconnect from local: Logged out (state=READY)
Oct 13 12:40:58 server postfix/lmtp[14723]: 5793E607700A: to=<snahmudov@snahmudov.net>, relay=server.snahmudov.net[private:dovecot-lmtp], delay=0.03, delays=0/0/0.01/0.01, dsn=2.0.0, status=sent (250 2.0.0 <snahmudov@snahmudov.net> s3F/Flrz7GtEOQAA@WRAUQ Saved)
Oct 13 12:40:58 server postfix/qmgr[14463]: 5793E607700A: removed
```

Рис. 3: Успешная доставка письма через LMTP

Настройка SMTP-аутентификации

```
10-master.conf  [--O] 18 L:[ 77+10  87/115] *(2064/2637b) 0010 0x00A
}

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 {
        mode = 0660
        user = postfix
        group = postfix
    }
}
```

Рис. 4: Настройка службы auth в Dovecot

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

Рис. 5: Тип аутентификации SASL и путь к сокету

Проверка через telnet

```
Installed:
  telnet-1:0.17-94.el10.x86_64

Complete!
[root@client.smahmudov.net ~]#
[root@client.smahmudov.net ~]# printf 'smahmudov\x00smahmudov\x00123456' | base64
c21haG11ZG92AHNtYWhtdWRvdgAxMjM0NTY=
[root@client.smahmudov.net ~]# telnet server.smahmudov.net 25
Trying 192.168.1.1...
Connected to server.smahmudov.net.
Escape character is '^]'.
220 server.smahmudov.net ESMTP Postfix
EHLO test
250-server.smahmudov.net
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN c21haG11ZG92AHNtYWhtdWRvdgAxMjM0NTY=
235 2.7.0 Authentication successful
```

Рис. 6: Проверка SMTP-аутентификации через telnet

Настройка SMTP over TLS

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

Рис. 7: TLS-сертификаты Dovecot и конфигурация Postfix

Настройка submission-порта

```
master.cf      [-M--] 0 L:[ 1+20 21/148] *(1113/7215b) 0032 0x020
#
# 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").
# -o smtpd_client_restrictions=
```

```
0090 - 3b 7a 45 a9 d2 c6 f1 b8-8b 6d 6f 4f 75 63 09 8c ;zE.....moOuc..
00a0 - 11 f6 9d ae 52 4a e1 b8-59 ed e8 cf 67 8d e4 a7 ....RJ..Y...g...
00b0 - 38 5a 0b 2e e2 2d 3c 2b-30 8c 03 18 f7 35 32 fc 8Z...-<+0....52.
00c0 - 21 80 40 c4 cf 41 4c 0c-47 f0 e2 8d 7a 9c bd f5 !.@..AL.G...z...
```

```
Start Time: 1760361424
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.smahmudov.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN c21haG11ZG92AHNtYWhtdWRvdgAxMjM0NTY=
235 2.7.0 Authentication successful
```

Результаты и вывод

Настроена полноценная почтовая инфраструктура, обеспечивающая защищённую передачу и аутентификацию пользователей.

Работоспособность подтверждена успешной доставкой писем и корректной работой через клиента **Evolution**.