

# **Отчёт по лабораторной работе 10**

**Расширенные настройкиSMTP-сервера**

Суннатилло Махмудов

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Теоретические сведения</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
3.1	Настройка LMTP в Dovecot . . . . .	8
3.2	Настройка SMTP-аутентификации . . . . .	12
3.3	Настройка SMTP over TLS . . . . .	17
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>23</b>
4.1	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	23
<b>5</b>	<b>Вывод</b>	<b>25</b>
<b>6</b>	<b>Контрольные вопросы</b>	<b>26</b>
<b>7</b>	<b>Список литературы</b>	<b>27</b>

# Список иллюстраций

3.1	Добавление протокола LMTP в конфигурацию Dovecot . . . . .	9
3.2	Настройка сервиса LMTP и Unix-сокета . . . . .	10
3.3	Изменение формата имени пользователя для аутентификации . .	10
3.4	Отправка тестового письма через LMTP . . . . .	11
3.5	Фрагмент лога успешной доставки сообщения через LMTP . . . . .	11
3.6	Проверка доставки письма на сервере . . . . .	12
3.7	Определение службы аутентификации в Dovecot . . . . .	14
3.8	Настройка SASL-аутентификации в Postfix . . . . .	14
3.9	Включение SMTP-аутентификации в master.cf . . . . .	16
3.10	Проверка SMTP-аутентификации через telnet . . . . .	17
3.11	Настройка TLS в Postfix и копирование сертификатов . . . . .	18
3.12	Внесение изменений для SMTP submission (порт 587) . . . . .	19
3.13	Проверка аутентификации по TLS через openssl . . . . .	20
3.14	Настройка SMTP с шифрованием в почтовом клиенте Evolution . .	21
3.15	Успешная отправка письма через защищённый SMTP . . . . .	21
3.16	Фрагмент лога успешной доставки письма через SMTP over TLS . .	22
4.1	Скрипт для сервера . . . . .	23
4.2	Скрипт для клиента . . . . .	24

## **Список таблиц**

# 1 Цель работы

Приобретение практических навыков по конфигурированию SMTP-сервера в части настройки аутентификации.

## 2 Теоретические сведения

Почтовая система в Linux строится на взаимодействии нескольких компонентов, каждый из которых выполняет определённую функцию в процессе передачи, хранения и получения электронных сообщений.

Основу системы составляют два ключевых сервера — **Postfix** и **Dovecot**.

**Postfix** — это почтовый транспортный агент (MTA, Mail Transfer Agent), который отвечает за приём, маршрутизацию и доставку электронной почты.

Он реализует протокол **SMTP (Simple Mail Transfer Protocol)**, обеспечивающий передачу сообщений между серверами.

Postfix также может выполнять функции **Relay-сервера**, пересылая почту между доменами, и поддерживает аутентификацию пользователей через **SASL (Simple Authentication and Security Layer)**.

**Dovecot** — это сервер почтовых ящиков (MDA, Mail Delivery Agent) и IMAP/POP3-сервер, обеспечивающий доступ пользователей к их сообщениям.

Он принимает почту от Postfix через протокол **LMTP (Local Mail Transfer Protocol)** и сохраняет её в каталоге почтового ящика пользователя, чаще всего в формате **Maildir**.

Dovecot также реализует механизмы аутентификации пользователей и шифрования с помощью **TLS (Transport Layer Security)**.

Для обеспечения безопасного обмена почтой между клиентом и сервером применяется протокол **SMTP over TLS**, который шифрует данные на уровне транспортного соединения, предотвращая перехват логинов, паролей и содержимого сообщений.

TLS использует сертификаты, позволяющие серверу подтвердить подлинность своей личности.

В процессе работы почтовой системы различают следующие основные порты и протоколы: - **25/tcp** — SMTP, используется для пересылки писем между серверами; - **143/tcp** — IMAP, обеспечивает работу с почтовыми сообщениями на сервере; - **110/tcp** — POP3, позволяет загружать письма на клиентское устройство; - **587/tcp** — Submission, используется клиентами для отправки почты с обязательным шифрованием (STARTTLS); - **993/tcp** и **995/tcp** — защищённые версии IMAPS и POP3S соответственно.

## 3 Выполнение лабораторной работы

### 3.1 Настройка LMTP в Dovecot

1. На виртуальной машине **server** был выполнен вход под пользователем и переход в режим суперпользователя:

```
sudo -i
```

В отдельном терминале запущен мониторинг почтовой службы:

```
tail -f /var/log/maillog
```

2. В конфигурационном файле **/etc/dovecot/dovecot.conf** был добавлен протокол **lmtp** в список поддерживаемых Dovecot протоколов.

После изменения параметр приобрёл вид:

```
protocols = imap pop3 lmtp
```



```
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 lmtpl

# 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
```

Рис. 3.1: Добавление протокола LMTP в конфигурацию Dovecot

3. В файле **/etc/dovecot/conf.d/10-master.conf** был настроен сервис **lmtpl** для взаимодействия с Postfix.

Добавлена следующая конфигурация:

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

Эта настройка определяет Unix-сокет, через который Postfix передаёт сообщения Dovecot, а также права доступа и владельца.

```
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. 3.2: Настройка сервиса LMTP и Unix-сокета

4. В файле **/etc/dovecot/conf.d/10-auth.conf** изменён формат имени пользователя для аутентификации.

Теперь он задаётся без доменной части:

`auth_username_format = %Ln`

```
10-auth.conf [----] 26 L:[ 35+17 52/130] *(2503/5249b) 0010 0x00A
# List of allowed characters in username. If the user-given username contains
# a character not listed in here, the login automatically fails. This is just
# an extra check to make sure user can't exploit any potential quote escaping
# vulnerabilities with SQL/LDAP databases. If you want to allow all characters,
# set this value to empty.
#auth_username_chars = abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890.-_@

# Username character translations before it's looked up from databases. The
# value contains series of from -> to characters. For example "#@/@" means
# 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
```

Рис. 3.3: Изменение формата имени пользователя для аутентификации

5. Для перенаправления локальной доставки через LMTP был выполнен пост-конфиг:

```
postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'
```

6. После внесённых изменений службы **Postfix** и **Dovecot** были перезапущены:

```
systemctl restart postfix
```

```
systemctl restart dovecot
```

7. С клиента, находящегося в домене **smahmudov.net**, отправлено тестовое письмо:

```
echo . | mail -s "LMTP test" smahmudov@smahmudov.net
```

```
[smahmudov@client.smahmudov.net ~]$ echo . | mail -s "LMTP test" smahmudov@smahmu  
dov.net  
[smahmudov@client.smahmudov.net ~]$ █
```

Рис. 3.4: Отправка тестового письма через LMTP

8. В журнале почтового сервера наблюдалась корректная передача сообщения от клиента через Postfix к Dovecot по LMTP.

Из лога видно, что сообщение было успешно сохранено в почтовый ящик получателя:

```
status=sent (250 2.0.0 smahmudov@smahmudov.net s3F/FLrz7GiEQAA0WRAUQ  
Saved)
```

```
Oct 13 12:40:58 server postfix/smtpd[14717]: connect from client.smahmudov.net[192.168.1.30]  
Oct 13 12:40:58 server postfix/smtpd[14717]: 5793E607700A: client=client.smahmudov.net[192.168.1.30]  
Oct 13 12:40:58 server postfix/cleanup[14721]: 5793E607700A: message-id=<20251013124058.4B3F6273D0@client.smahmudov.net>  
Oct 13 12:40:58 server postfix/smtpd[14717]: disconnect from client.smahmudov.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=<smahmudov@client.smahmudov.net>, size=550, nrcpt=1 (queue active)  
Oct 13 12:40:58 server postfix/local[14722]: 5793E607700A: passing <smahmudov@smahmudov.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(smahmudov)<14724><s3F/FLrz7GiEQAA0WRAUQ>: msgid=<20251013124058.4B3F6273D0@client.smahmudov.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=<smahmudov@smahmudov.net>, relay=server.smahmudov.net[private/dovecot-lmtp], delay=0.03, delays=  
0/0/0.01/0.01, dsn=2.0.0, status=sent (250 2.0.0 <smahmudov@smahmudov.net> s3F/FLrz7GiEQAA0WRAUQ Saved)  
Oct 13 12:40:58 server postfix/qmgr[14463]: 5793E607700A: removed
```

Рис. 3.5: Фрагмент лога успешной доставки сообщения через LMTP

9. Проверка почтового ящика на сервере подтвердила получение тестового письма:

```
MAIL=~/.Maildir/ mail
```

В списке сообщений присутствует письмо с темой **“LMTP test”**, доставленное от клиента.

```
[smahmudov@server.smahmudov.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.24.  Type '?' for help
/home/smahmudov/Maildir: 2 messages 1 new
  1 smahmudov          2025-10-10 05:29   18/651   "test1
►N  2 smahmudov@client.sma 2025-10-13 12:40   21/834   "LMTP test
&
[-- Message  2 -- 21 lines, 834 bytes --]:
Date: Mon, 13 Oct 2025 12:40:58 +0000
To: smahmudov@smahmudov.net
Subject: LMTP test
Message-Id: <20251013124058.4B3F6273D0@client.smahmudov.net>
From: smahmudov@client.smahmudov.net

.

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

Рис. 3.6: Проверка доставки письма на сервере

## 3.2 Настройка SMTP-аутентификации

1. В файле **/etc/dovecot/conf.d/10-master.conf** была определена служба аутентификации пользователей.

Конфигурация включает два unix-сокета:

```
service auth {
  unix_listener auth-userdb {
    mode = 0600
    user = dovecot
  }
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }
}
```

```
}  
}
```

Пояснение к настройке:

- **service auth** — определяет службу аутентификации в Dovecot.
- **unix\_listener auth-userdb** — внутренний сокет Dovecot для обращения собственных сервисов.
- **mode = 0600** — разрешения доступа только владельцу.
- **user = dovecot** — владелец сокета — системный пользователь Dovecot.
- **unix\_listener /var/spool/postfix/private/auth** — сокет для взаимодействия с Postfix.
- **mode = 0660** — разрешения на доступ пользователю и группе.
- **user = postfix, group = postfix** — предоставляют Postfix право использовать этот сокет.

```
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. 3.7: Определение службы аутентификации в Dovecot

2. Для Postfix был задан тип аутентификации SASL и путь к соответствующему unix-сокету:

`postconf -e 'smtpd_sasl_type = dovecot'`

`postconf -e 'smtpd_sasl_path = private/auth'`

```
[root@server.smahmudov.net ~]#
[root@server.smahmudov.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.smahmudov.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.smahmudov.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.smahmudov.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'
```

Рис. 3.8: Настройка SASL-аутентификации в Postfix

3. Для ограничения приёма почты и предотвращения использования сервера в качестве релейа были заданы ограничения получателей:

`postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'`

Комментарии к опциям:

- **reject\_unknown\_recipient\_domain** — отклоняет письма с неизвестными доменами получателей.
  - **permit\_mynetworks** — разрешает приём сообщений от доверенных сетей, определённых в mynetworks.
  - **reject\_non\_fqdn\_recipient** — запрещает использование неполных (неполных FQDN) адресов.
  - **reject\_unauth\_destination** — предотвращает пересылку писем для внешних доменов (анти-релей).
  - **reject\_unverified\_recipient** — проверяет существование получателя перед приёмом письма.
  - **permit** — разрешает приём после прохождения всех проверок.
4. Для ограничения диапазона доверенной сети Postfix было выполнено:  
`postconf -e 'mynetworks = 127.0.0.0/8'`
  5. Для тестирования аутентификации в файле **/etc/postfix/master.cf** была включена возможность авторизации через SASL.  
 Активирована строка для smtp-сервиса:  
`smtp inet n - n - - smtpd`  
`-o smtpd_sasl_auth_enable=yes`  
`-o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain`

```
master.cf      [-M--] 0 L:[ 7*28 35/148] *(1824/7217b) 0035 0x023
#
# =====
# 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=
# -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
# Choose one: enable submissions for loopback clients only, or for any client.
1help    2save    3mark    4Replac  5Copy    6Move    7Search  8Delete  9
```

Рис. 3.9: Включение SMTP-аутентификации в master.cf

6. После настройки службы **Postfix** и **Dovecot** были перезапущены:

```
systemctl restart postfix
```

```
systemctl restart dovecot
```

7. На клиентской машине был установлен пакет **telnet** для тестирования соединения:

```
dnf -y install telnet
```

8. С помощью команды `printf` была сгенерирована строка для аутентификации пользователя **smahmudov** с паролем **123456** в кодировке base64:

```
printf 'smahmudov\x00smahmudov\x00123456' | base64
```

Результат:

```
c21haG11ZG92AHNtYWhtdWRvdkAxMjMONTY=
```

9. Подключение к SMTP-серверу и проверка успешной аутентификации:

```
telnet server.smahmudov.net 25
```

```
EHLO test
```

```
AUTH PLAIN c21haG11ZG92AHNtYWhtdWRvdkAxMjMONTY=
```



Сервер вернул ответ:

**235 2.7.0 Authentication successful**, что подтверждает корректную настройку SMTP-аутентификации.

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

Complete!
[root@client.smahmudov.net ~]#
[root@client.smahmudov.net ~]# printf 'smahmudov\x00smahmudov\x00123456' | base64
c21haG11ZG92AHNtYWhtdWRvdGxMjM0NTY=
[root@client.smahmudov.net ~]# telnet server.smahmudov.net 25
Trying 192.168.1.1...
Connected to server.smahmudov.net.
Escape character is '^J'.
220 server.smahmudov.net ESMTP Postfix
EHLO test
250-server.smahmudov.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN c21haG11ZG92AHNtYWhtdWRvdGxMjM0NTY=
235 2.7.0 Authentication successful
```

Рис. 3.10: Проверка SMTP-аутентификации через telnet

### 3.3 Настройка SMTP over TLS

1. На сервере был настроен TLS с использованием временного сертификата, выданного **Dovecot**.

Для предотвращения ошибок SELinux файлы сертификата и ключа были скопированы в стандартные каталоги TLS:

```
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs/
```

```
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private/
```

После этого в Postfix были указаны пути к сертификату и ключу, а также параметры кеширования TLS-сессий и уровень безопасности:

```
postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
```

```
postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
```

```
postconf -e 'smtpd_tls_session_cache_database=btree:/var/lib/postfix/smtpd_scache'
postconf -e 'smtpd_tls_security_level=may'
postconf -e 'smtp_tls_security_level=may'
```

```
[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. 3.11: Настройка TLS в Postfix и копирование сертификатов

2. Для активации SMTP на порту **587** (submission) в файле **/etc/postfix/master.cf** были внесены следующие изменения.

Исходная запись для smtp была упрощена до:

```
smtp inet n - n - - smtpd
```

И добавлен новый блок для службы **submission**:

```
submission inet n - n - - smtpd
```

```
-o smtpd_tls_security_level=encrypt
```

```
-o smtpd_sasl_auth_enable=yes
```

```
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain
```

Таким образом, сервер принимает соединения на порту 587 с обязательным шифрованием и аутентификацией пользователей.

```
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=
1Help      2Save      3Mark      4Replac    5Copy      6Mov
```

Рис. 3.12: Внесение изменений для SMTP submission (порт 587)

3. Для разрешения работы службы **smtp-submission** был настроен межсетевой экран:

```
firewall-cmd --add-service=smtp-submission
```

```
firewall-cmd --add-service=smtp-submission --permanent
```

```
firewall-cmd --reload
```

4. После внесённых изменений служба Postfix была перезапущена:

```
systemctl restart postfix
```

5. С клиента было выполнено тестовое подключение к SMTP-серверу через порт **587** с использованием шифрования STARTTLS:

```
openssl s_client -starttls smtp -crlf -connect server.smahmudov.net:587
```

После установления защищённого соединения были выполнены команды:

EHLO test

AUTH PLAIN c21haG11ZG92AHNtYWhtdWRvdgAxMjMONTY=

Сервер подтвердил успешную аутентификацию:

### 235 2.7.0 Authentication successful

```
0090 - 3b 7a 45 a9 d2 c6 f1 b8-8b 6d 6f 4f 75 63 09 8c ;zE.....mo0uc..
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-VRIFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN c21haG11ZG92AHNtYWhtdWRvdgAxMjMONTY=
235 2.7.0 Authentication successful
```

Рис. 3.13: Проверка аутентификации по TLS через openssl

6. В почтовом клиенте **Evolution** были настроены параметры отправки почты через SMTP:

- Сервер: *mail.smahmudov.net*
- Порт: **587**
- Метод шифрования: *STARTTLS after connecting*
- Тип аутентификации: *PLAIN*

- Имя пользователя: *smahmudov*

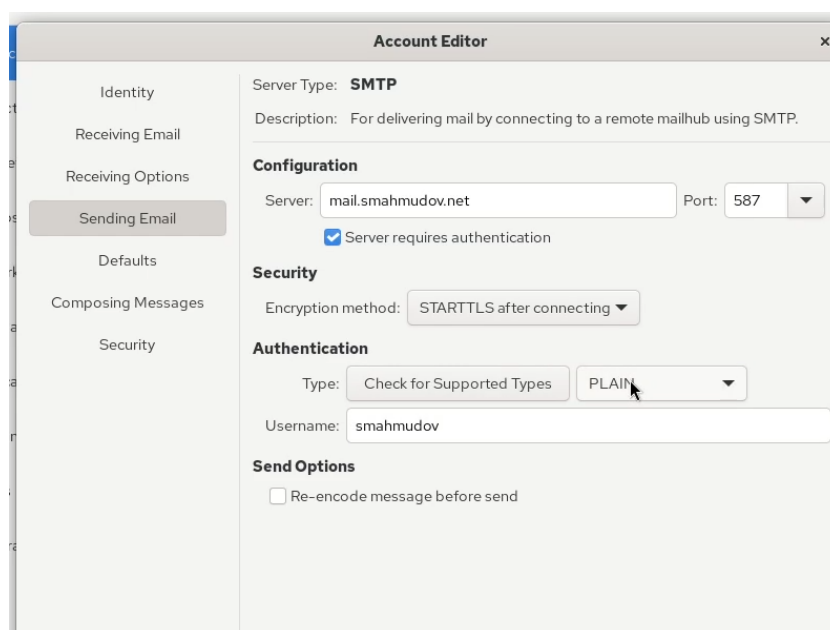


Рис. 3.14: Настройка SMTP с шифрованием в почтовом клиенте Evolution

7. После настройки был выполнен тест отправки письма.

Сообщение с темой **“test hello”** было успешно доставлено в почтовый ящик получателя, что подтверждает корректную работу SMTP over TLS.

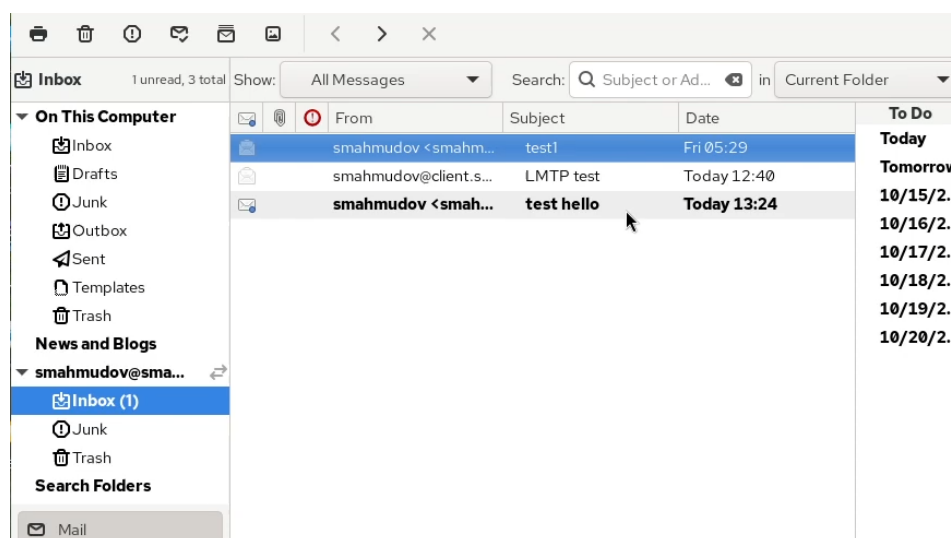


Рис. 3.15: Успешная отправка письма через защищённый SMTP

8. В логе почтового сервера видно, что соединение установлено с использованием шифрования TLS и успешной аутентификации пользователя.

Письмо было передано через Postfix и доставлено Dovecot в папку INBOX:

**status=sent (250 2.0.0 smahmudov@smahmudov.net Saved mail to INBOX)**

```
Oct 13 13:24:32 server postfix/smtpd[19573]: connect from client.smahmudov.net[192.168.1.30]
Oct 13 13:24:32 server postfix/tlsgr[19575]: warning: btree:/var/lib/postfix/smtpd_scache is unavailable. unsupported dictionary type: btree
Oct 13 13:24:36 server postfix/smtpd[19573]: 0EDDB607700A: client=client.smahmudov.net[192.168.1.30], sasl_method=PLAIN, sasl_username=smahmudov
Oct 13 13:24:36 server postfix/cleanup[20511]: 0EDDB607700A: message-id=<5d7d4cfc444eb50b615d3646f0c659fac90ca4c4.camel@smahmudov.net>
Oct 13 13:24:36 server postfix/qmgr[19550]: 0EDDB607700A: from=<smahmudov@smahmudov.net>, size=560, nrcpt=1 (queue active)
Oct 13 13:24:36 server postfix/smtpd[19573]: disconnect from client.smahmudov.net[192.168.1.30] ehlo=2 starttls=1 auth=1 mail=1 rcpt=1 data=1 quit=1 commands=8
Oct 13 13:24:36 server postfix/local[20512]: 0EDDB607700A: passing <smahmudov@smahmudov.net> to transport=lmp
Oct 13 13:24:36 server dovecot[16504]: lmp(20514): Connect from local
Oct 13 13:24:36 server dovecot[16504]: lmp(smahmudov)<20514><GFxYBJT97GgiUAAA0WRAUQ>: msgid=<5d7d4cfc444eb50b615d3646f0c659fac90ca4c4.camel@smahmudov.net>: saved mail to INBOX
Oct 13 13:24:36 server postfix/lmp[20513]: 0EDDB607700A: to=<smahmudov@smahmudov.net>, relay=server.smahmudov.net[private/dovecot-lmp], delay=0.02, delays=0.01/0.01/0, dsn=2.0.0, status=sent (250 2.0.0 <smahmudov@smahmudov.net> GFxYBJT97GgiUAAA0WRAUQ Saved)
Oct 13 13:24:36 server dovecot[16504]: lmp(20514): Disconnect from local: Logged out (state=READY)
Oct 13 13:24:36 server postfix/qmgr[19550]: 0EDDB607700A: removed
Oct 13 13:24:46 server dovecot[16504]: imap-login: Login: user=<smahmudov>, method=PLAIN, rip=192.168.1.30, lip=192.168.1.1, mpid=20549, TLS, session=<wEHuMApBcMjAqAEe>
```

Рис. 3.16: Фрагмент логa успешной доставки письма через SMTP over TLS

## 4 Выполнение лабораторной работы

### 4.1 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. В подкаталог **mail/etc/dovecot/** были скопированы актуальные конфигурационные файлы Dovecot:
2. В скрипт **/vagrant/provision/server/mail.sh** были внесены изменения, обеспечивающие автоматическую установку и настройку сервисов **Postfix**, **Dovecot**, и необходимых инструментов.

```
10 restorecon -vR /etc
11 echo "Configure firewall"
12 firewall-cmd --add-service smtp --permanent
13 firewall-cmd --add-service pop3 --permanent
14 firewall-cmd --add-service pop3s --permanent
15 firewall-cmd --add-service imap --permanent
16 firewall-cmd --add-service imaps --permanent
17 firewall-cmd --add-service smtp-submission --permanent
18 firewall-cmd --reload
19 echo "Start postfix service"
20 systemctl enable postfix
21 systemctl start postfix
22 echo "Configure postfix"
23 postconf -e 'mydomain = smahmudov.net'
24 postconf -e 'myorigin = $mydomain'
25 postconf -e 'inet_protocols = ipv4'
26 postconf -e 'inet_interfaces = all'
27 postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain'
28 #postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'
29 echo "Configure postfix for dovecot"
30 postconf -e 'home_mailbox = Maildir/'
31 echo "Configure postfix for auth"
32 postconf -e 'smtpd_sasl_type = dovecot'
33 postconf -e 'smtpd_sasl_path = private/auth'
34 postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_unauth_destination'
35 postconf -e 'mynetworks = 127.0.0.0/8'
36 echo "Configure postfix for SMTP over TLS"
37 cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
38 cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
39 postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
40 postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
41 postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
42 postconf -e 'smtpd_tls_security_level = may'
43 postconf -e 'smtp_tls_security_level = may'
44 postfix set-permissions
45 restorecon -vR /etc
46 systemctl stop postfix
47 systemctl start postfix
48 systemctl restart dovecot
```

Рис. 4.1: Скрипт для сервера

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y install postfix
5  dnf -y install s-nail
6  dnf -y install evolution telnet
7
8  echo "Configure postfix"
9  postconf -e 'inet_protocols = ipv4'
10 echo "Start postfix service"
11 systemctl enable postfix
12 systemctl start postfix
```

Рис. 4.2: Скрипт для клиента



## 5 Вывод

В ходе лабораторной работы была выполнена полная настройка почтового сервера с поддержкой **LMTP**, **SMTP-аутентификации** и **SMTP over TLS**.

Были сконфигурированы службы **Postfix** и **Dovecot**, обеспечены защищённая передача данных и авторизация пользователей.

Почтовый обмен успешно проверен с помощью клиента **Evolution** и инструментов **telnet** и **openssl**, подтверждающая корректную работу системы.

## 6 Контрольные вопросы

1. **Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.**

Формат аутентификации с указанием домена задаётся в файле `/etc/dovecot/conf.d/10-auth.conf` параметром:

```
auth_username_format = %Lu
```

Здесь `%L` приводит имя пользователя к нижнему регистру, а `%u` означает полный логин вместе с доменом (например, `user@smahmudov.net`).

2. **Какие функции выполняет почтовый Relay-сервер?**

Почтовый Relay-сервер (или SMTP Relay) выполняет передачу почтовых сообщений между различными почтовыми доменами и серверами.

Он принимает почту от отправителя и перенаправляет её к следующему узлу сети или к серверу назначения, обеспечивая доставку сообщений за пределами локального домена.

3. **Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?**

Если почтовый сервер настроен как открытый Relay (Open Relay), им могут воспользоваться злоумышленники для рассылки спама или фишинговых сообщений.

Это приведёт к попаданию IP-адреса сервера в «чёрные списки» (RBL), снижению репутации домена и блокировке легитимных почтовых отправок.

## 7 Список литературы

1. Postfix SASL Howto. — URL: [http://www.postfix.org/SASL\\_README.html](http://www.postfix.org/SASL_README.html) (visited on 09/13/2021).