Отчёт по лабораторной работе 10

Расширенные настройки SMTP-сервера

Сейдалиев Тагиетдин Ровшенович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Выполнение

2.1 Настройка LMTP в Dovecot

Для включения поддержки протокола LMTP был изменён файл `dovecot.conf`, где в параметр `protocols` добавлен `lmtp`. Это обеспечивает возможность приёма сообщений от Postfix через локальный LMTP-сокет.

```
## 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
```

Рис. 2.1: Добавление протокола LMTP в Dovecot

В файле `10-master.conf` был переопределён сервис `lmtp`. В конфигурации указано расположение Unix-сокета, через который Postfix передаёт сообщения, а также заданы права доступа и принадлежность к пользователю и группе `postfix`.

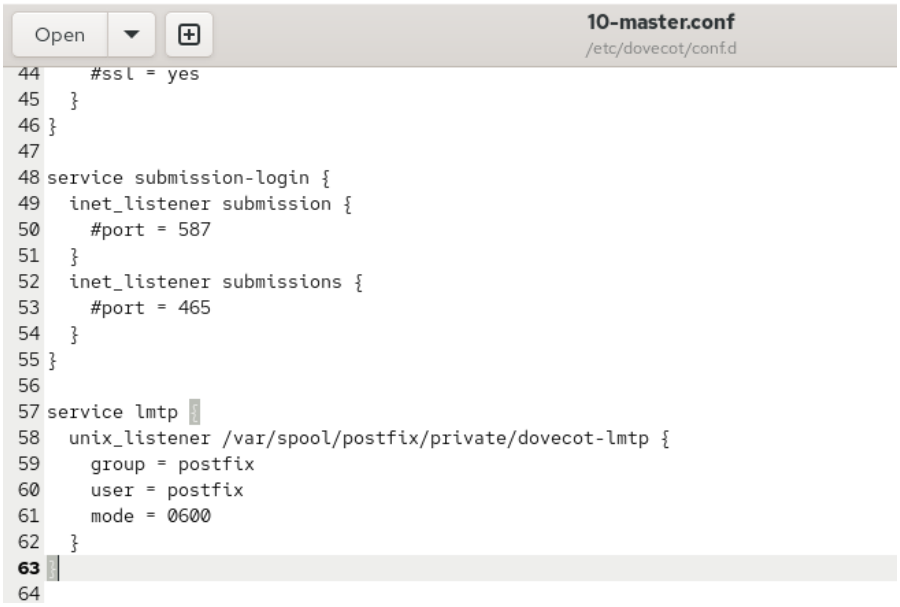


Рис. 2.2: Настройка сервиса LMTP в 10-master.conf

В файле `10-auth.conf` задано использование локальной части логина без доменной части. Это позволяет корректно сопоставлять имя пользователя с его локальной учётной записью.

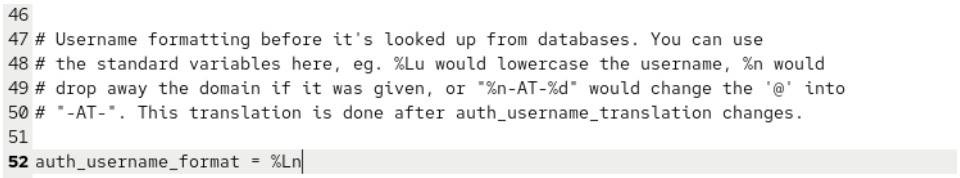


Рис. 2.3: Настройка auth_username_format

Postfix был перенастроен на передачу сообщений не напрямую, а через LMTP-сокет Dovecot. После внесения изменений службы Postfix и Dovecot были перезапущены для применения конфигурации.

При отправке тестового письма в журнале фиксировались следующие этапы:

- приём письма Postfix от клиента;
- передача сообщения локальному транспортному агенту;
- вызов LMTP-доставки через сокет `/var/spool/postfix/private/dovecot-lmtp`;

- подтверждение Dovecot о сохранении сообщения в INBOX;
- отчёт Postfix об успешной доставке.

```
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.trseidalie
v.net>
Nov 30 11:11:18 server postfix/smtpd[24038]: disconnect from client.trseidaliev.net[192.168.1.30] ehlo=2 starttls=1 ma
il=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=<20251130081116.9483623
68984@client.trseidaliev.net>: saved mail to INBOX
Nov 30 11:11:18 server postfix/lmtp[24044]: 19F35239C170: to=<trseidaliev@trseidaliev.net>, relay=server.trseidaliev.n
et[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@trseidal
iev.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. 2.4: Логи доставки письма через LMTP

Пояснение по логам:

Передача письма успешно прошла по цепочке: клиент → Postfix → LMTP → Dovecot.

Ключевая строка `saved mail to INBOX` подтверждает корректную доставку, а статус `250 2.0.0` — успешное завершение транзакции.

Просмотр содержимого почтового ящика пользователя подтвердил наличие тестового письма, доставленного через LMTP.

```
[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]$
```

Рис. 2.5: Просмотр Maildir пользователя

Письмо успешно доставлено, что подтверждает корректную интеграцию Postfix и Dovecot через LMTP.

2.2 Настройка SMTP-аутентификации

В файле `10-master.conf` была добавлена конфигурация службы `auth`, обеспечивающая взаимодействие Postfix и Dovecot при проверке пользовательских учетных данных.

```
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     grpup = postfix
92     user = postfix
93     mode = 0660
94   }
95
96   # Auth process is run as this user.
97   #user = $default_internal_user
98 }
```

Рис. 2.6: Фрагмент настройки службы auth

Построчное пояснение:

- `service auth {` — начало блока настроек службы аутентификации Dovecot.
- `unix_listener auth-userdb {` — настройка сокета, через который внутренние процессы Dovecot получают информацию о пользователях.
- `mode = 0600` — доступ только для владельца сокета.
- `user = dovecot` — владельцем сокета является пользователь `dovecot`.
- `}` — закрытие блока `auth-userdb`.
- `unix_listener /var/spool/postfix/private/auth {` — сокет, используемый Postfix для SASL-аутентификации через Dovecot.

- `group = postfix` — группа владельца сокета — `postfix`, что позволяет Postfix обращаться к нему.
- `user = postfix` — владельцем сокета является пользователь Postfix.
- `mode = 0660` — разрешение на чтение и запись для владельца и группы.
- `}` — закрытие блока Postfix-сокета.
- `}` — завершение определения службы `auth`.

В Postfix была включена поддержка SASL-аутентификации через Dovecot и указан путь к соответствующему сокету.

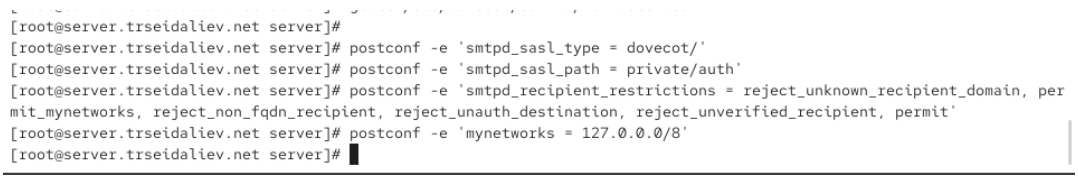


Рис. 2.7: Настройка параметров SASL через postconf

В настройках Postfix заданы параметры, регулирующие приём писем:

- `reject_unknown_recipient_domain` — отклоняет письма, если домен получателя не существует.
- `permit_mynetworks` — разрешает приём писем от доверенных IP-адресов.
- `reject_non_fqdn_recipient` — отклоняет адреса получателя без полного доменного имени.
- `reject_unauth_destination` — запрещает использовать сервер как открытый релей; принимает письма только для локальных доменов.
- `reject_unverified_recipient` — отклоняет письма, если проверка существования пользователя невозможна или неуспешна.
- `permit` — разрешает обработку после прохождения всех предыдущих проверок.

Эти параметры предотвращают использование сервера в качестве SMTP-relay и обеспечивают проверку корректности адресов.

В Postfix адрес доверенной сети ограничен только локальным хостом:

`mynetworks = 127.0.0.0/8`

Это гарантирует, что сервер принимает письма без аутентификации только от самого себя.

В файле `master.cf` в определении службы SMTP добавлены параметры:

- включение SASL-аутентификации (`smtpd_sasl_auth_enable=yes`);
- изменение ограничений получателей для разрешения авторизованных пользователей (`permit_sasl_authenticated`).

```
#
# 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=
#  -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.
#127.0.0.1:submissions inet n  -       n       -       -       smtpd
#submissions     inet  n       -       n       -       -       smtpd
```

Рис. 2.8: Фрагмент master.cf с изменёнными параметрами

Для проверки работы аутентификации на клиентской машине было установлено средство `telnet`, а затем сгенерирована строка авторизации формата base64.

После подключения к серверу:

- сервер сообщает поддерживаемые расширения SMTP;

- выполняется команда `EHLO test`;
- производится проверка аутентификации командой `AUTH PLAIN <строка>`.

На скриншоте показано успешное прохождение аутентификации:

```
[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
221 2.0.0 Bye
Connection closed by foreign host.
[root@client.trseidaliev.net ~]#
```

Рис. 2.9: Проверка авторизации через telnet

Сервер вернул код `235 2.7.0 Authentication successful`, подтверждающий корректную работу SMTP-аутентификации.

2.3 Настройка SMTP over TLS

Для настройки TLS использовались временные сертификаты Dovecot. Файлы сертификата и ключа были перенесены в системные каталоги `/etc/pki/tls/certs` и `/etc/pki/tls/private` для корректной работы SELinux.

На скриншоте видно выполнение копирования и настройку Postfix путём указания сертификата, приватного ключа, каталога кеширования TLS-сессий, а также

уровня безопасности:

```
[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. 2.10: Копирование сертификатов и настройка параметров TLS в Postfix

После внесения параметров Postfix начинает принимать TLS-соединения и использовать шифрование при работе по SMTP.

Для запуска SMTP-сервиса с поддержкой TLS и аутентификации на 587-м порту в файл `master.cf` были внесены изменения.

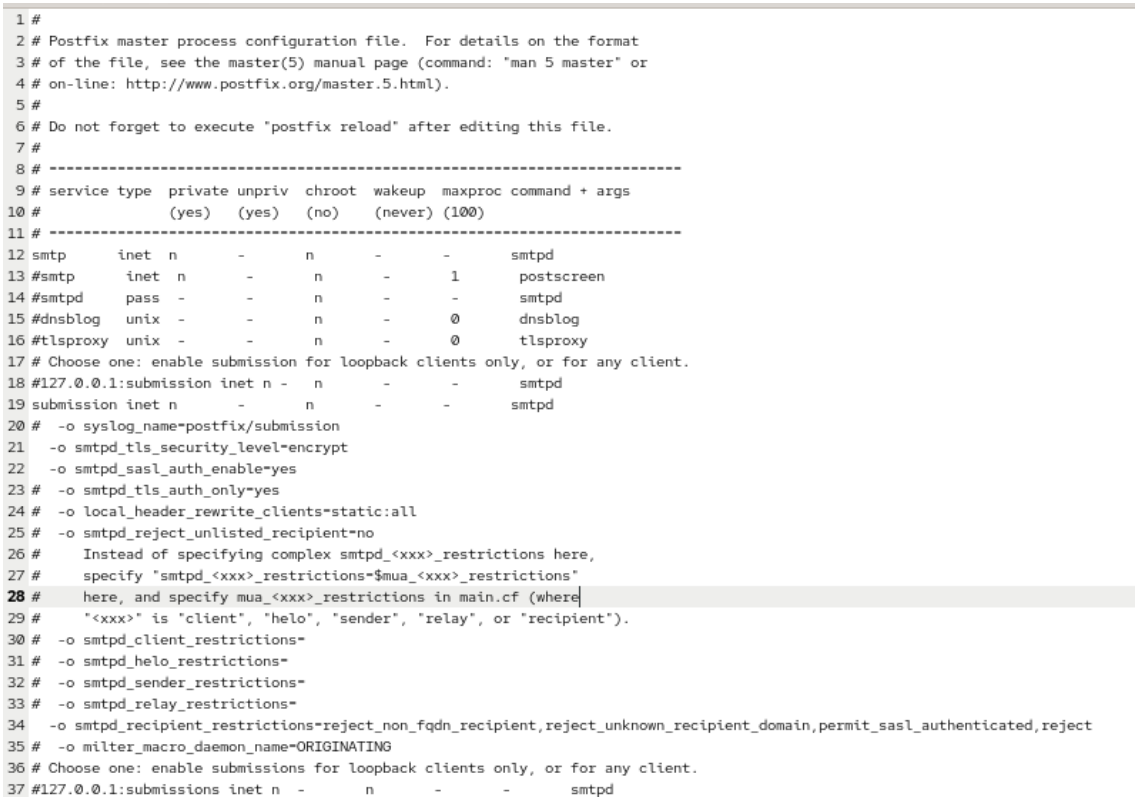
Основной SMTP-сервис на порту 25 оставлен в минимальной конфигурации:

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

Добавлена новая служба submission:

- работает на порту 587;
- требует применение шифрования (опция `encrypt`);
- включает SASL-аутентификацию;
- использует ограничивающие правила для адресов получателя, предотвращающие open relay.

Фрагмент изменённого файла:



```
#
# 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=
#  -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.
#127.0.0.1:submissions inet n  -       n       -       -       smtpd
```

Рис. 2.11: Изменения в master.cf для службы submission

Чтобы разрешить работу службы smtp-submission, в firewall были добавлены соответствующие правила. Сервис стал доступен и после перезагрузки конфигурации межсетевой экран учитывает постоянное разрешение.

С клиента выполнялось подключение к SMTP-серверу по порту 587 с использованием STARTTLS:

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

После установления защищённого канала были выполнены:

- команда EHLO;
- попытка аутентификации через механизм AUTH PLAIN.

Скриншот демонстрирует успешную TLS-сессию и подтверждённую аутентификацию:

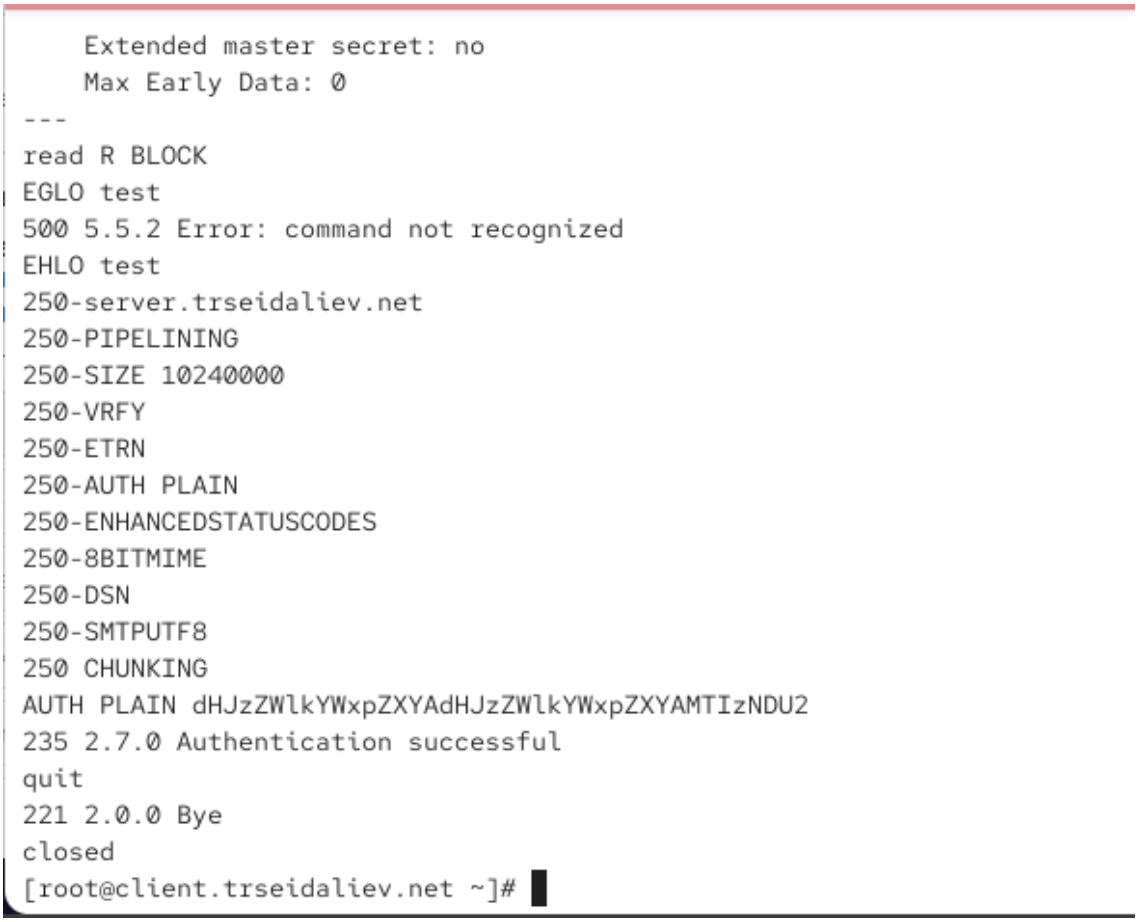


Рис. 2.12: Проверка SMTP over TLS через openssl и telnet

В почтовом клиенте Evolution был настроен SMTP-сервер со следующими параметрами:

- порт: 587;
- метод шифрования: STARTTLS;
- тип аутентификации: PLAIN.

Настройки отображены на скриншоте:

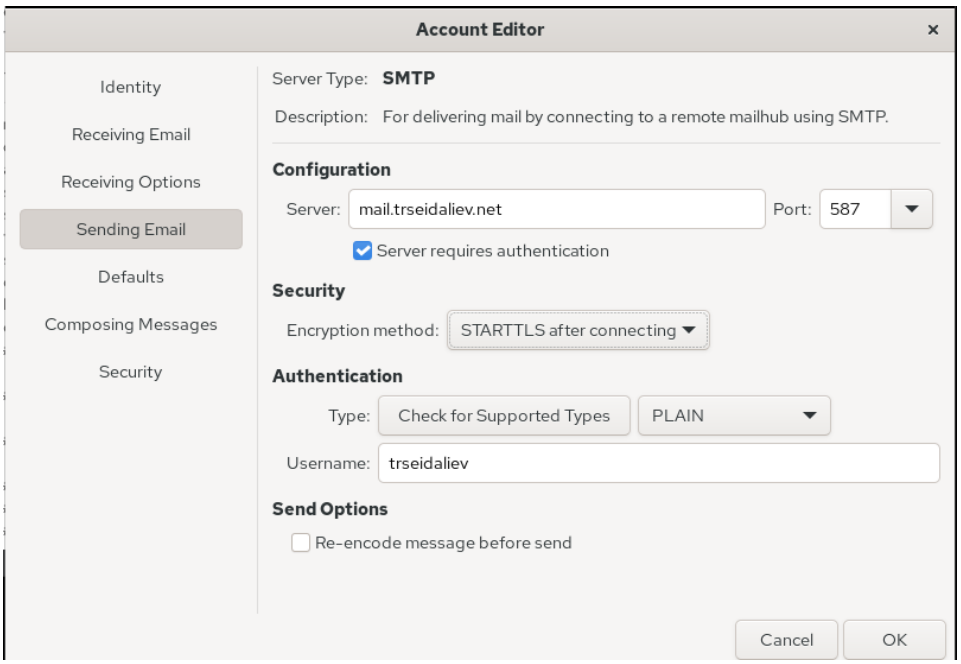


Рис. 2.13: Настройки SMTP в Evolution

После настройки почтовые сообщения успешно отправлялись через TLS-защищённый SMTP-канал.

В клиентском интерфейсе Evolution отображаются входящие письма, отправленные через TLS-канал. Все они доставлены корректно:

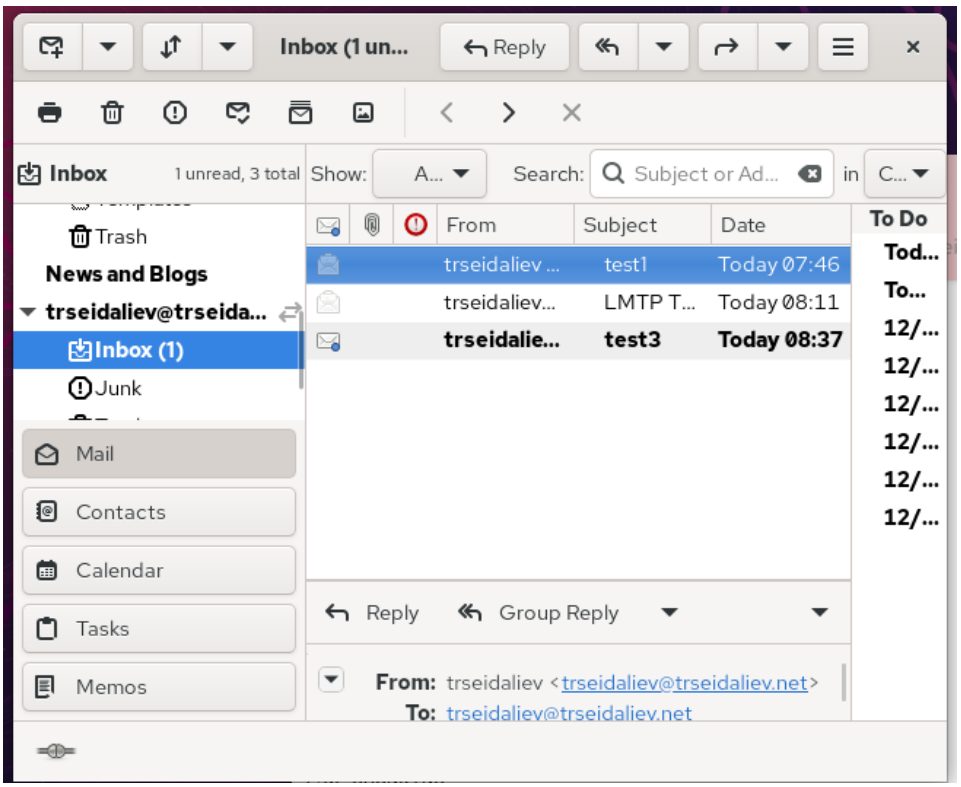


Рис. 2.14: Полученные письма в Evolution

Мониторинг `/var/log/maillog` показал корректную работу цепочки:

1. клиент → Postfix (через TLS);
2. передача сообщения в LMTP-службу;
3. Dovecot принимает письмо и сохраняет его в INBOX;
4. Postfix подтверждает успешную доставку.

Логи демонстрируют успешную аутентификацию и использование LMTP для хранения почты:

```
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=lmtp
Nov 30 11:37:28 server dovecot[26635]: lmtp(27929): Connect from local
Nov 30 11:37:28 server dovecot[26635]: lmtp(trseidaliev)<27929><7WmsA0gCLGkZbQAAe9wJyQ>: msgid=<c1450906964e3baa8d5dbc
1785f9972d067c20cd.camel@trseidaliev.net>: saved mail to INBOX
Nov 30 11:37:28 server dovecot[26635]: lmtp(27929): Disconnect from local: Logged out (state=READY)
Nov 30 11:37:28 server postfix/lmtp[27928]: 0BD2523AD265: to=<trseidaliev@trseidaliev.net>, relay=server.trseidaliev.n
et[private/dovecot-lmtp], 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
```

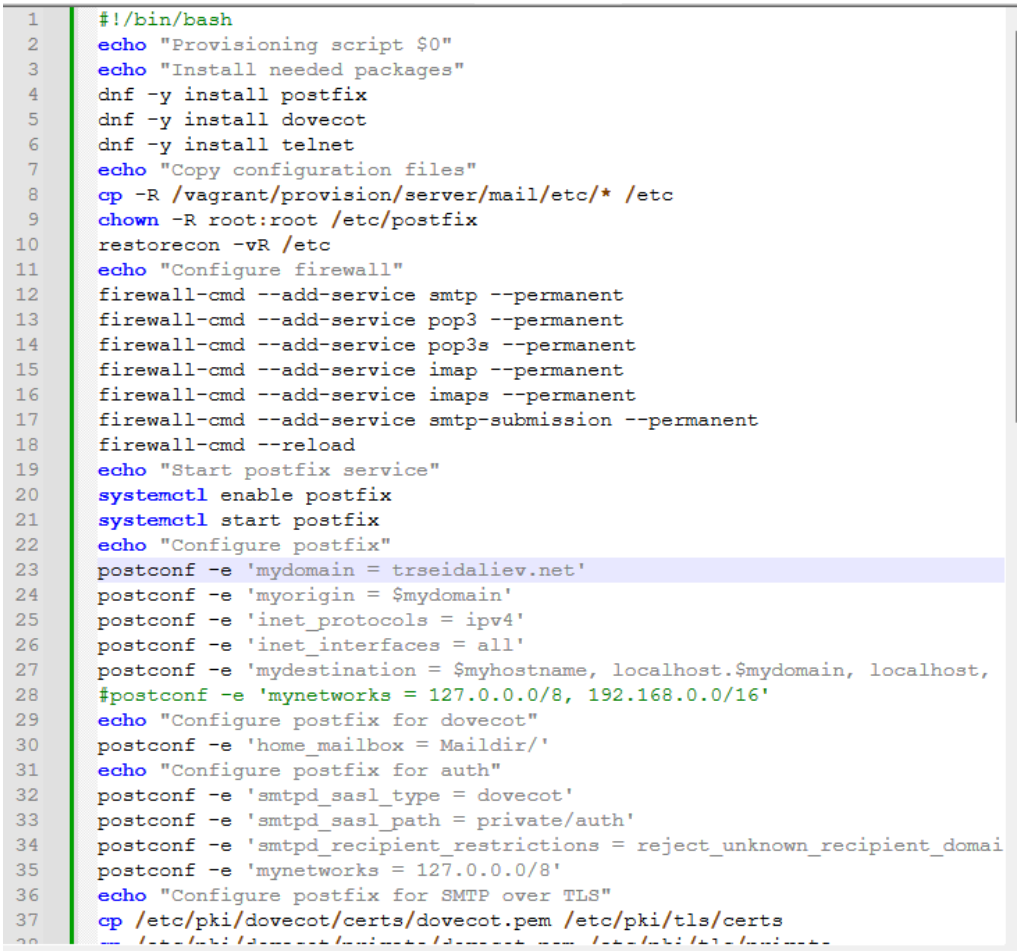
Рис. 2.15: Фрагмент логов Postfix и Dovecot

2.4 Внесение изменений в конфигурацию внутреннего окружения

Для сохранения всех модификаций в инфраструктуре Vagrant были перенесены обновлённые конфигурации в каталог `/vagrant/provision/server/`.

Скрипт `mail.sh` был дополнен параметрами для расширенной настройки SMTP и TLS.

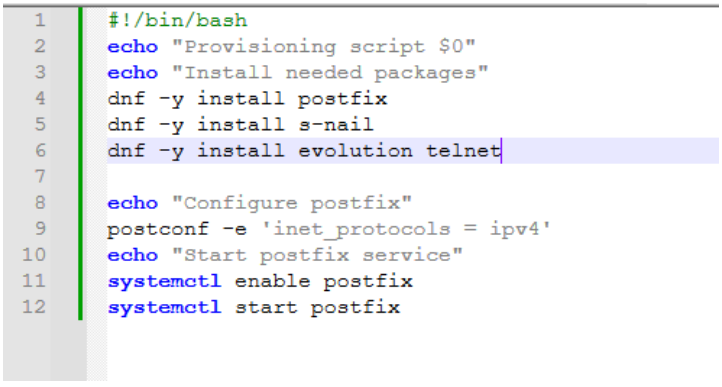
Пример фрагмента обновлённого скрипта:



```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install postfix
dnf -y install dovecot
dnf -y install telnet
echo "Copy configuration files"
cp -R /vagrant/provision/server/mail/etc/* /etc
chown -R root:root /etc/postfix
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-service smtp --permanent
firewall-cmd --add-service pop3 --permanent
firewall-cmd --add-service pop3s --permanent
firewall-cmd --add-service imap --permanent
firewall-cmd --add-service imaps --permanent
firewall-cmd --add-service smtp-submission --permanent
firewall-cmd --reload
echo "Start postfix service"
systemctl enable postfix
systemctl start postfix
echo "Configure postfix"
postconf -e 'mydomain = trseidaliev.net'
postconf -e 'myorigin = $mydomain'
postconf -e 'inet_protocols = ipv4'
postconf -e 'inet_interfaces = all'
postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost,
#postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'
echo "Configure postfix for dovecot"
postconf -e 'home_mailbox = Maildir/'
echo "Configure postfix for auth"
postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'
postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domai
postconf -e 'mynetworks = 127.0.0.0/8'
echo "Configure postfix for SMTP over TLS"
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
```

Рис. 2.16: Часть обновлённого provisioning-скрипта

Дополнительно создан вариант минимального provisioning-скрипта для клиента, включающий установку Evolution и telnet:



```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install postfix
dnf -y install s-nail
dnf -y install evolution telnet

echo "Configure postfix"
postconf -e 'inet_protocols = ipv4'
echo "Start postfix service"
systemctl enable postfix
systemctl start postfix
```

Рис. 2.17: Минимальный provisioning-скрипт для клиента

3 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.

4 Контрольные вопросы

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

Для использования полного адреса электронной почты (логин + домен) можно задать:

```
auth_username_format = %n@%d
```

В этом случае Dovecot будет ожидать логин в виде `user@domain`, не отбрасывая доменную часть.

4.2 2. Какие функции выполняет почтовый Relay-сервер?

Почтовый Relay-сервер выполняет следующие задачи:

- принимает письма от отправителей и передаёт их другому серверу SMTP для дальнейшей доставки;
- маршрутизирует почтовый трафик между доменами и почтовыми системами;
- может использоваться как промежуточный узел для фильтрации, антивирусной проверки или балансировки нагрузки;

- обеспечивает доставку сообщений в случае временной недоступности конечного сервера, помещая почту в очередь.

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

Неправильно настроенный Relay-сервер представляет серьёзную угрозу:

- **Использование как open relay** — злоумышленники смогут рассылать спам через сервер без ограничений.
- **Включение в чёрные списки (RBL)** — провайдеры и другие почтовые сервера начнут блокировать почту с данного домена/узла.
- **Повышенная нагрузка на сервер** — массовая спам-рассылка быстро исчерпает ресурсы системы.
- **Компрометация доверия к домену** — почта домена будет расцениваться как вредоносная, что приведёт к блокировкам и ухудшению доставки.
- **Риск DoS-атак** — спам-боты могут перегрузить очереди обработки писем.

Поэтому строгие ограничения (`reject_unauth_destination`, `permit_mynetworks`, `permit_sasl_authenticated`) обязательны для защиты SMTP-сервера.