Лабораторная работа №10

Расширенные настройки SMTP-сервераФайл

Спелов Андрей Николаевич

Содержание

1 Цель работы **6**

2 Выполнение лабораторной работы **7**

3 Выводы **20**

4 Ответы на контрольные вопросы: **21**

Список литературы **23**

Список иллюстраций

2.1 Запуск в дополнительном терминале мониторинга работы почтовой службы. 7
2.2 Добавление в список протоколов, с которыми может работать Dovecot, протокола LMTP. 8
2.3 Настройка в Dovecot сервиса lmtp для связи с Postfix. 8
2.4 Переопределение в Postfix с помощью postconf передачи сообщений не на прямую, а через заданный unix-сокет. 9
2.5 Настройка в файле /etc/dovecot/conf.d/10-auth.conf формата имени пользователя для аутентификации в форме логина пользователя без указания домена. 9
2.6 Перезапуск Postfix и Dovecot. 9
2.7 Отправка из-под учётной записи своего пользователя письма с клиента. 9
2.8 Просмотр содержания логов при мониторинге почтовой службы. 10
2.9 Просмотр на сервере почтового ящика пользователя. 10
2.10 Определение в файле /etc/dovecot/conf.d/10-master.conf службы аутентификации пользователей. 11
2.11 Настройка для Postfix типа аутентификации SASL для smtpd и пути к соответствующему unix-сокету, настройка Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины, ограничение в настройках Postfix приёма почты только локальным адресом SMTP-сервера сети. 12
2.12 Временный запуск для проверки работы аутентификации SMTP-сервера (порт 25) с возможностью аутентификации. 12
2.13 Перезапуск Postfix и Dovecot. 12
2.14 Установка на клиенте telnet. 13
2.15 Получение на клиенте строки для аутентификации, подключение на клиенте к SMTP-серверу посредством telnet, тестирование соединения, проверка авторизации и завершение сессии telnet на клиенте. 14
2.16 Настройка на сервере TLS и предварительное копирование необходимых файлов сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги. Настройка конфигурации Postfix. 15
2.17 Замена строк в файле /etc/postfix/master.cf для того чтобы запустить SMTP-сервер на 587-м порту. 15

2.18 Настройка межсетевого экрана, разрешив работать службе smtp-submission. 16
2.19 Перезапуск Postfix. 16
2.20 Подключение на клиенте к SMTP-серверу через 587-й порт посредством openssl, тестирование подключения по telnet и проверка аутентификации. 17
2.21 Корректирование настроек почтового клиента Evolution. 18
2.22 Переход в каталог на виртуальной машине server для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и помещение в соответствующие подкаталоги конфигурационных файлов Dovecot и Postfix. 18
2.23 Внесение соответствующих изменений по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh. . . . 19
2.24 Внесение изменения в файл /vagrant/provision/client/mail.sh. . . . 19

Список таблиц

1 Цель работы

Целью данной работы является приобретение практических навыков по конфигурированию SMTP-сервера в части настройки аутентификации.

2 Выполнение лабораторной работы

На виртуальной машине server войдём под нашим пользователем и откроем терминал. Перейдём в режим суперпользователя.В дополнительном терминале запустим мониторинг работы почтовой службы.(рис. 2.1).

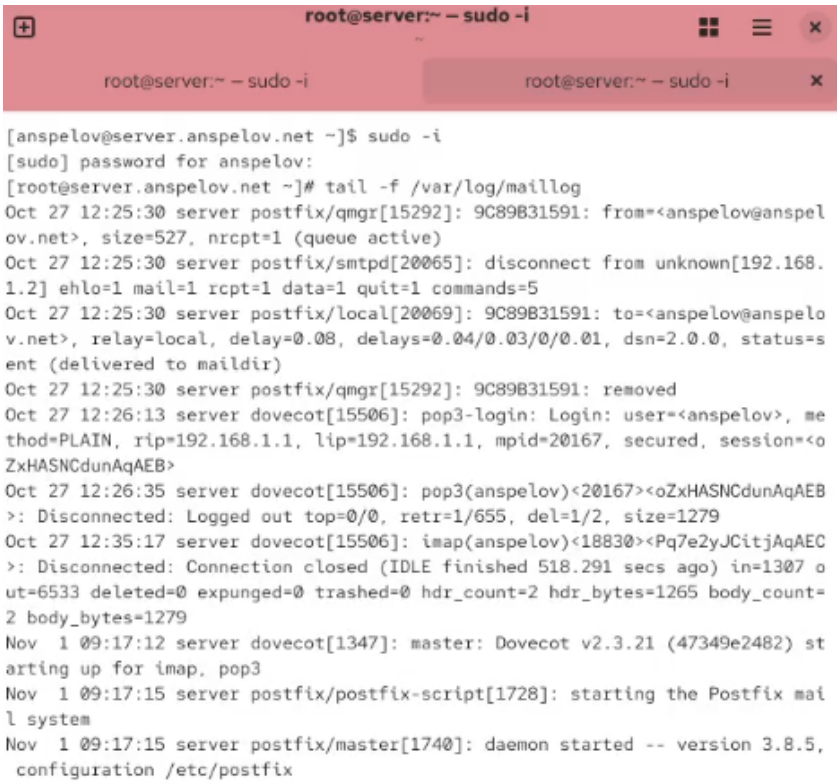

Рис. 2.1: Запуск в дополнительном терминале мониторинга работы почтовой службы.

Добавим в список протоколов, с которыми может работать Dovecot, протокол LMTP. (рис. 2.2).

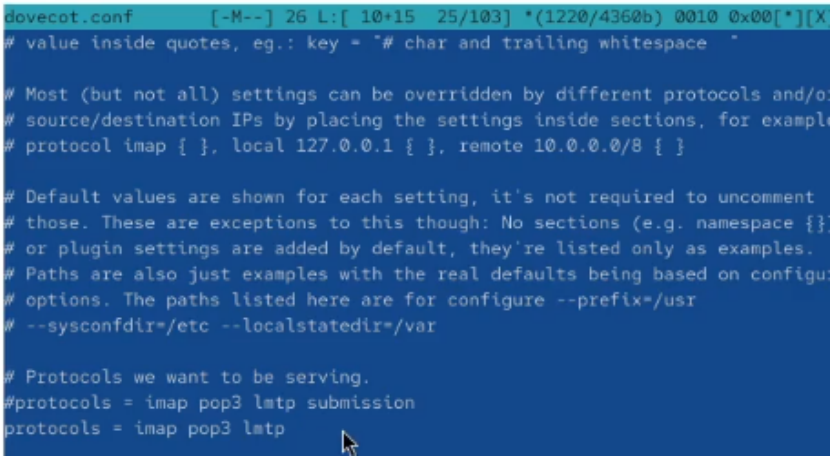

Рис. 2.2: Добавление в список протоколов, с которыми может работать Dovecot, протокола LMTP.

Настроим в Dovecot сервис lmtp для связи с Postfix. Для этого в файле /etc/dovecot/conf.d/10-master.conf замените определение сервиса lmtp на следующую запись из лабораторной работы. Эта запись определяет расположение файла с описанием прослушиваемого unix-сокета, а также задаёт права доступа к нему и определяет принадлежность к группе и пользователю postfix.(рис. 2.3).

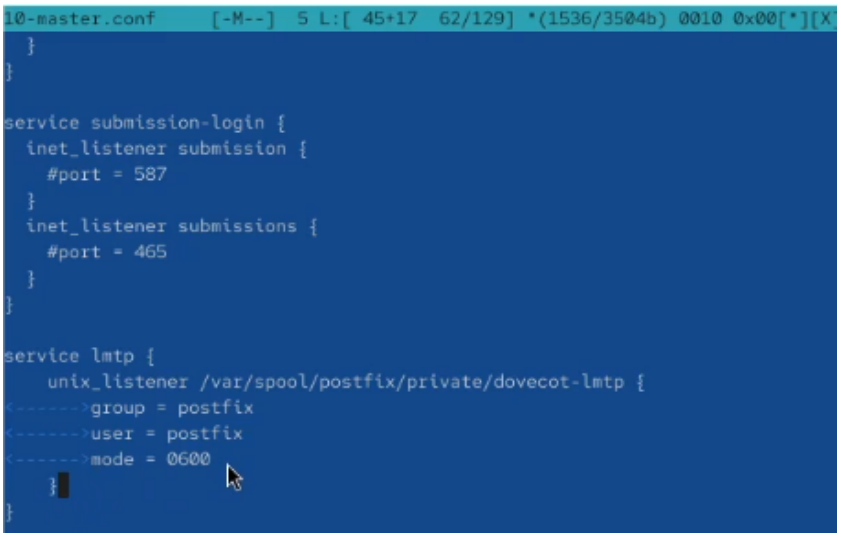

Рис. 2.3: Настройка в Dovecot сервиса lmtp для связи с Postfix.

Переопределим в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокет(рис. 2.4).

```
[root@server.anspelov.net ~]# postconf -e 'mailbox_transport = lmtp:unix:priv
ate/dovecot-lmtp'
[root@server.anspelov.net ~]#
```

Рис. 2.4: Переопределение в Postfix с помощью postconf передачи сообщений не на прямую, а через заданный unix-сокет.

В файле /etc/dovecot/conf.d/10-auth.conf зададим формат имени пользователя для аутентификации в форме логина пользователя без указания домена (рис. 2.5).

```
# 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 '@' in
# "-AT-". This translation is done after auth_username_translation changes.
auth_username_format = %Ln
```

Рис. 2.5: Настройка в файле /etc/dovecot/conf.d/10-auth.conf формата имени пользователя для аутентификации в форме логина пользователя без указания домена.

Перезапустим Postfix и Dovecot (рис. 2.6).

```
[root@server.anspelov.net ~]# systemctl restart postfix
[root@server.anspelov.net ~]# systemctl restart dovecot
[root@server.anspelov.net ~]#
```

Рис. 2.6: Перезапуск Postfix и Dovecot.

Из-под учётной записи своего пользователя отправим письмо с клиента (рис. 2.7).

```
anspelov@client:~
[anspelov@client.anspelov.net ~]$ echo .| mail -s "LMTP test" anspelov@anspel
ov.net
[anspelov@client.anspelov.net ~]$
```

Рис. 2.7: Отправка из-под учётной записи своего пользователя письма с клиента.

После чего посмотрим содержание логов при мониторинге почтовой службы(рис. 2.8).

Рис. 2.8: Просмотр содержания логов при мониторинге почтовой службы.

На сервере просмотрим почтовый ящик пользователя (рис. 2.9).

```
[root@server.anspelov.net ~]# MAIL=~/Maildir/ mail
```

Рис. 2.9: Просмотр на сервере почтового ящика пользователя.

В файле /etc/dovecot/conf.d/10-master.conf определим службу аутентификации пользователей(рис. 2.10).

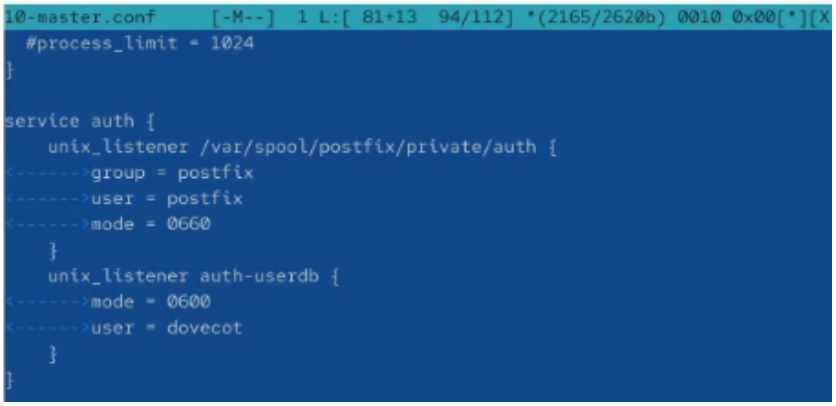

Рис. 2.10: Определение в файле /etc/dovecot/conf.d/10-master.conf службы аутентификации пользователей.

Для Postfix зададим тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету: postconf -e ‘smtpd_sasl_type = dovecot’ postconf -e ‘smtpd_sasl_path = private/auth’ Далее настроим Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины (имеется в виду локальных пользователейсервера), обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок (порядок указания опций имеет значение): postconf -e ‘smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit’ В настройках Postfix ограничим приём почты только локальным адресом SMTP-сервера сети(рис. 2.11).

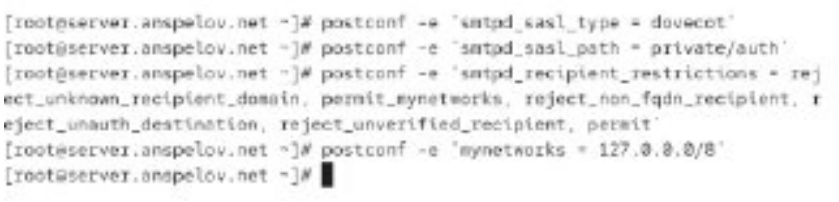

Рис. 2.11: Настройка для Postfix типа аутентификации SASL для smtpd и пути к соответствующему unix-сокету, настройка Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины, ограничение в настройках Postfix приёма почты только локальным адресом SMTP-сервера сети.

Для проверки работы аутентификации временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Для этого в файле /etc/postfix/master.cf заменим строку(рис. 2.12).

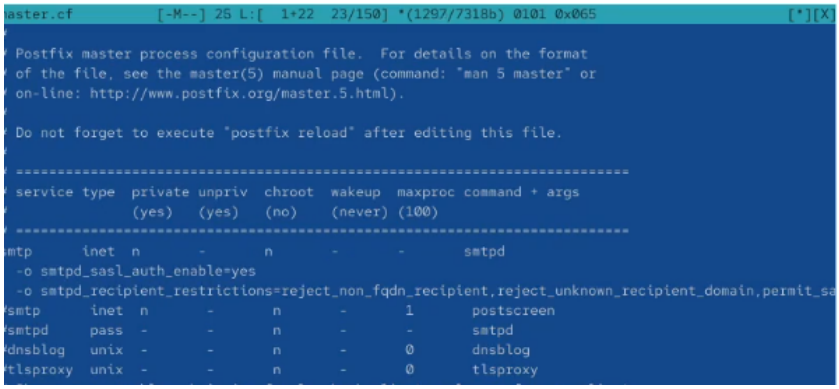

Рис. 2.12: Временный запуск для проверки работы аутентификации SMTP-сервера (порт 25) с возможностью аутентификации.

Затем перезапустим Postfix и Dovecot (рис. 2.13).

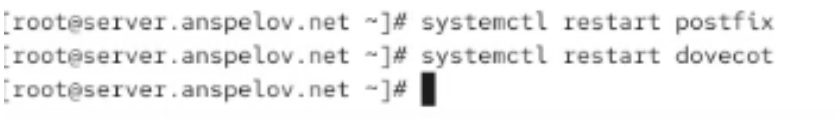

Рис. 2.13: Перезапуск Postfix и Dovecot.

На клиенте установим telnet(рис. 2.14).

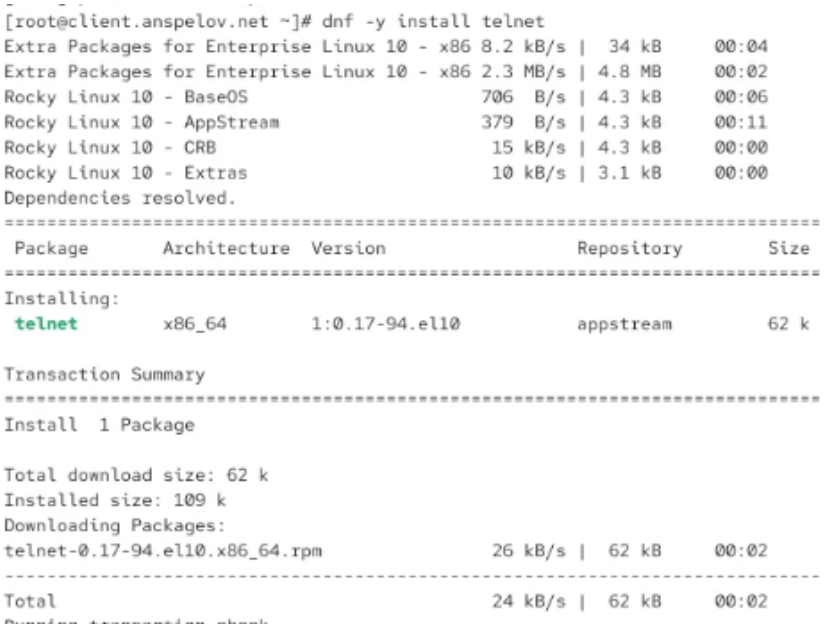

Рис. 2.14: Установка на клиенте telnet.

На клиенте получим строку для аутентификации. В качестве результата получим строку для аутентификации в формате base64. После чего подключимся на клиенте к SMTP-серверу посредством telnet: telnet server.anspelov.net 25 Теперь протестируем соединение, введя EHLO test и проверим авторизацию, задав: AUTH PLAIN Завершим сессию telnet на клиенте (рис. 2.15).

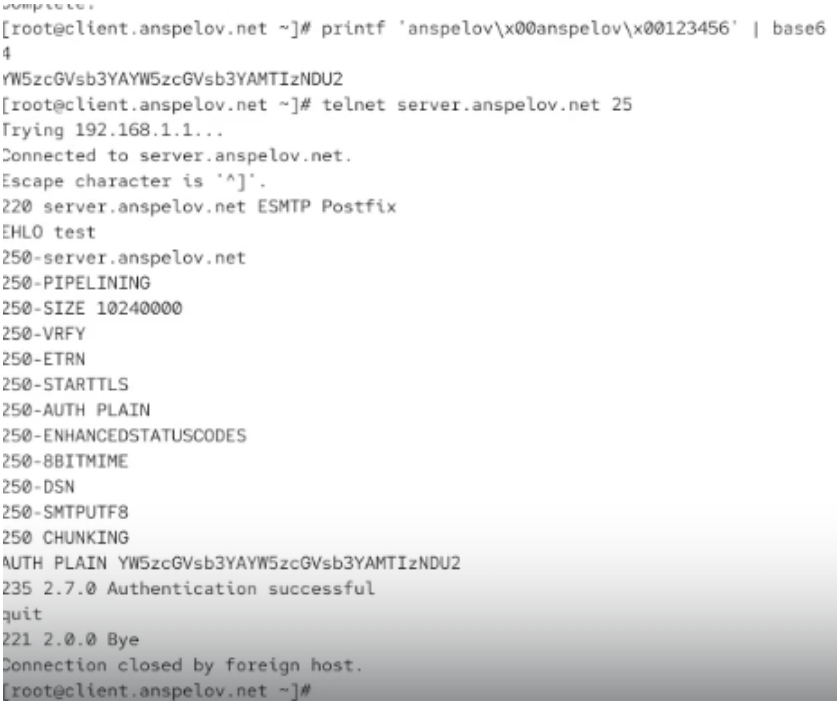

Рис. 2.15: Получение на клиенте строки для аутентификации, подключение на клиенте к SMTP-серверу посредством telnet, тестирование соединения, проверка авторизации и завершение сессии telnet на клиенте.

Настроим на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно скопируем необходимые файлы сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги (чтобы не было проблем с SELinux). Далее сконфигурируем Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности(рис. 2.16).

```
[root@server.anspelov.net ~]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls
/certs
[root@server.anspelov.net ~]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/t
ls/private
[root@server.anspelov.net ~]# postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/cert
s/dovecot.pem'
[root@server.anspelov.net ~]# postconf -e 'smtpd_tls_key_file=/etc/pki/tls/priva
te/dovecot.pem'
[root@server.anspelov.net ~]# postconf -e 'smtpd_tls_session_cache_database = bt
ree:/var/lib/postfix/smtpd_scache'
[root@server.anspelov.net ~]# postconf -e 'smtpd_tls_security_level = may'
[root@server.anspelov.net ~]# postconf -e 'smtp_tls_security_level = may'
[root@server.anspelov.net ~]#
```

Рис. 2.16: Настройка на сервере TLS и предварительное копирование необходимых файлов сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги. Настройка конфигурации Postfix.

Для того чтобы запустить SMTP-сервер на 587-м порту, в файле /etc/postfix/master.cf заменим строки(рис. 2.17).

```
master.cf          [-M--] 28 L:[  7+17  24/149] *(1336/7283b) 0115 0x073  [*][X]
#
# ==========================================================================
# 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_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recip
#  -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").
```

Рис. 2.17: Замена строк в файле /etc/postfix/master.cf для того чтобы запустить SMTP-сервер на 587-м порту.

Настроим межсетевой экран, разрешив работать службе smtp-submission (рис. 2.18).

Рис. 2.18: Настройка межсетевого экрана, разрешив работать службе smtp-submission.

Перезапустим Postfix (рис. 2.19).

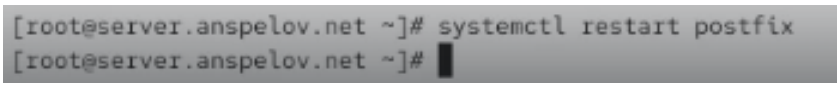

Рис. 2.19: Перезапуск Postfix.

На клиенте подключимся к SMTP-серверу через 587-й порт посредством openssl и протестируем подключение по telnet, проверим аутентификацию (рис. 2.20).

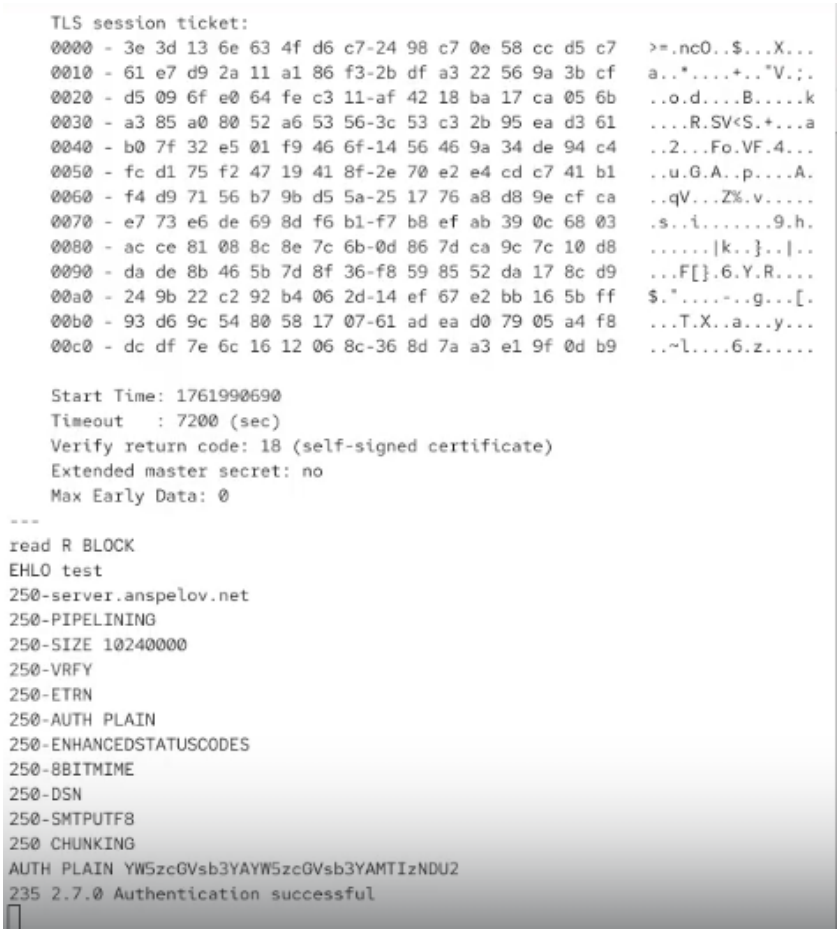

Рис. 2.20: Подключение на клиенте к SMTP-серверу через 587-й порт посредством openssl, тестирование подключения по telnet и проверка аутентификации.

Проверим корректность отправки почтовых сообщений с клиента посредством почтового клиента Evolution, предварительно скорректировав настройки учётной записи, а именно для SMTP-сервера укажем порт 587, STARTTLS и обычный пароль (рис. 2.21).

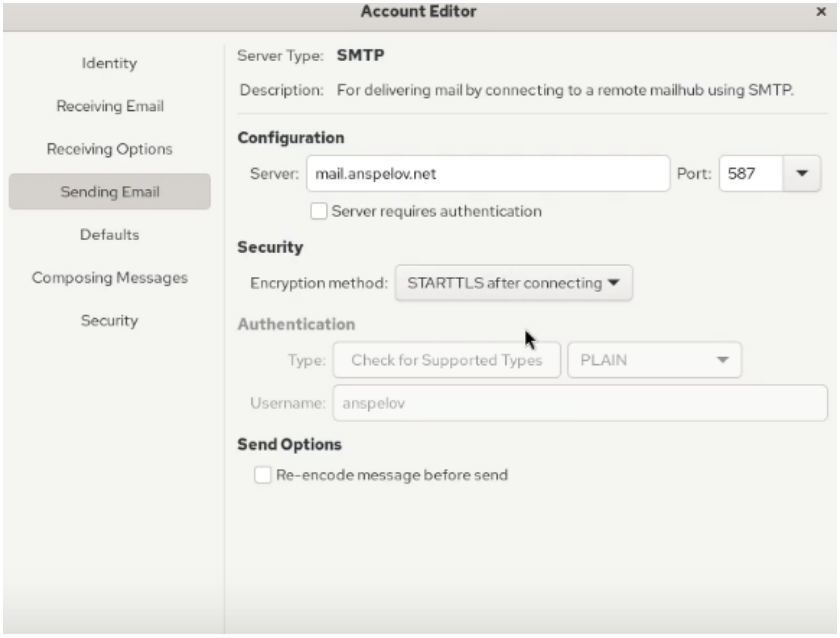

Рис. 2.21: Корректирование настроек почтового клиента Evolution.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/. В соответствующие подкаталоги поместим конфигурационные файлы Dovecot и Postfix (рис. 2.22).

```
[root@server.anspelov.net ~]# cd /vagrant/provision/server
[root@server.anspelov.net server]# cp -R /etc/dovecot/dovecot.conf /vagrant/prov
ision/server/mail/etc/dovecot/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/dovecot.conf'? Yes
[root@server.anspelov.net server]# cp -R /etc/dovecot/conf.d/10-master.conf /vag
rant/provision/server/mail/etc/dovecot/conf.d/
[root@server.anspelov.net server]# cp -R /etc/dovecot/conf.d/10-auth.conf /vagra
nt/provision/server/mail/etc/dovecot/conf.d/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/conf.d/10-auth.conf'?
Yes
[root@server.anspelov.net server]# mkdir -p /vagrant/provision/server/mail/etc/p
ostfix/
[root@server.anspelov.net server]# cp -R /etc/postfix/master.cf /vagrant/provisi
on/server/mail/etc/postfix/
[root@server.anspelov.net server]#
```

Рис. 2.22: Переход в каталог на виртуальной машине server для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и помещение в соответствующие подкаталоги конфигурационных файлов Dovecot и Postfix.

Внесём соответствующие изменения по расширенной конфигурации SMTP-

сервера в файл /vagrant/provision/server/mail.sh (рис. 2.23).

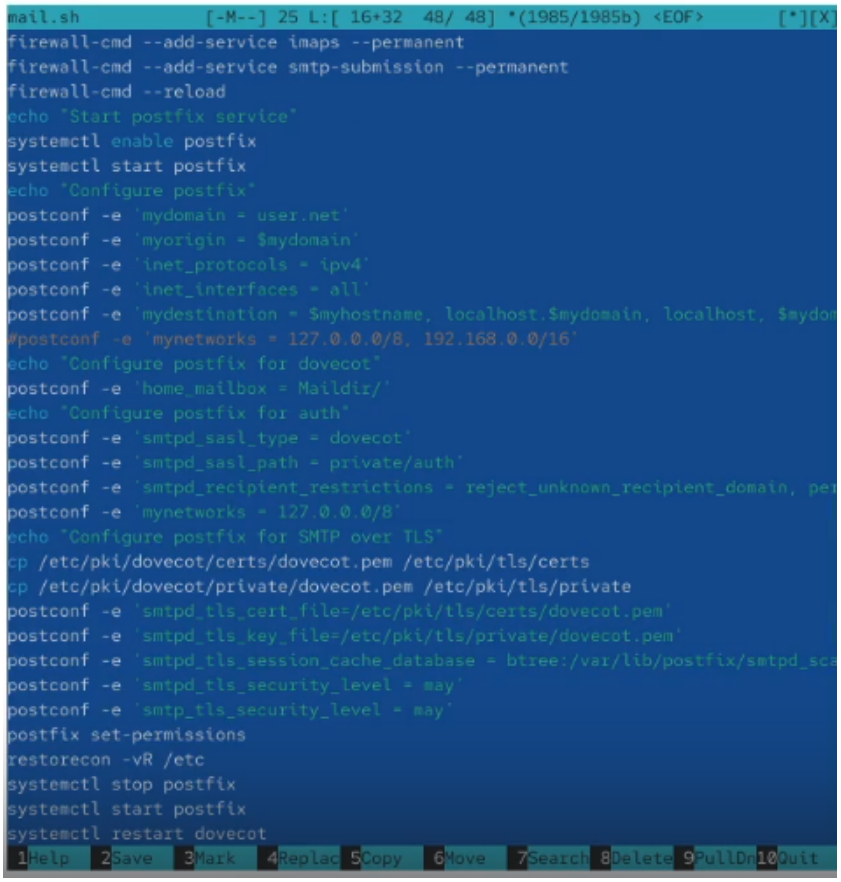

Рис. 2.23: Внесение соответствующих изменений по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh.

Внесём изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet (рис. 2.24).

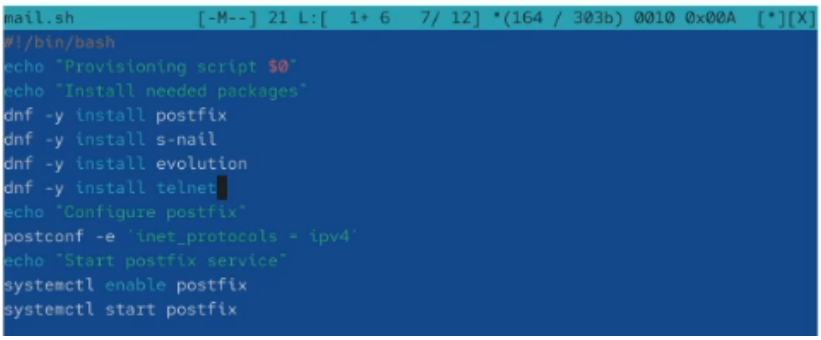

Рис. 2.24: Внесение изменения в файл /vagrant/provision/client/mail.sh.

3 Выводы

В ходе выполнения лабораторной работы были приобретены практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

4 Ответы на контрольные вопросы:

1. Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена. Допустим, у нас есть почтовый ящик с адресом user@example.com. В конфигурационном файле Dovecot (/etc/dovecot/conf.d/10-auth.conf), мы можем указать формат аутентификации следующим образом: auth_username_format = %Lu В этом примере %Lu означает, что аутентификация будет проходить в формате “user” без учета регистра букв. Если вам нужно учитывать домен, вы можете использовать %n: auth_username_format = %Ln Таким образом, при вводе логина “user@example.com” пользователь будет аутентифицироваться с именем пользователя “user” и доменом “example.com”.

2. Какие функции выполняет почтовый Relay-сервер? – Пересылка почты: Relay-сервер принимает почтовые сообщения от клиентов и пересылает их к адресатам. Это особенно полезно,если у вас нет прямого доступа к серверу назначения или если вы хотите централизованно управлять отправкой почты. Маршрутизация почты: Relay-сервер может определять наилучший маршрут для доставки почты на основе определенных правил и политик. Блокировка спама: Некоторые Relay-серверы выполняют функции фильтрации спама, блокируя нежелательные сообщения до их отправки на сервер назначения.

3. Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера? – Открытый Relay: Если сервер настроен как

открытый Relay, это может привести к злоупотреблению. Злоумышленники могут использовать сервер для отправки спама, что может повлечь за собой блокировку IP-адреса сервера или другие санкции. Спуфинг: Атаки, связанные с подделкой отправителя (спуфинг), могут быть использованы для маскировки настоящего источника почты. Это может быть проблемой, если сервер Relay доверяет внешним источникам без должной аутентификации. Отказ в обслуживании (DoS): Атаки типа DoS могут быть направлены на Relay-сервер, перегружая его запросами на пересылку почты и создавая неприемлемую загрузку.

Список литературы