**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

ОТЧЕТ

по лабораторной работе № 10

Дисциплина «Администрирование сетевых подсистем»

*Тема «Расширенные настройки SMTP-сервера»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

# Цель работы

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

# Задание

1. Настроить Dovecot для работы с LMTP.

2. Настроить аутентификацию посредством SASL на SMTP-сервере.

3. Настроить работу SMTP-сервера поверх TLS.

4.Скорректировать скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server.

**Выполнение**

**1. Настройка LMTP в Dovecote**

1. На виртуальной машине server вошла под своим пользователем и открыла терминал. Перешла в режим суперпользователя. В дополнительном терминале запустила мониторинг работы почтовой службы.

2. Добавила в список протоколов, с которыми может работать Dovecot, протокол LMTP (рис.1.1).

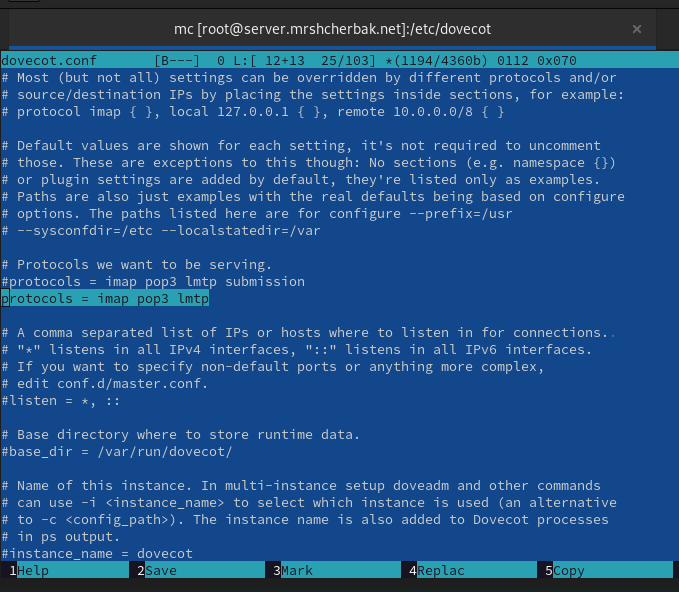


Рис.1.1. Редактирование файла /etc/dovecot/dovecot.conf

3. Настроила в Dovecot сервис lmtp для связи с Postfix. Для этого в файле /etc/dovecot/conf.d/10-master.conf заменила определение сервиса lmtp на запись, представленную на рис.1.2. 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.

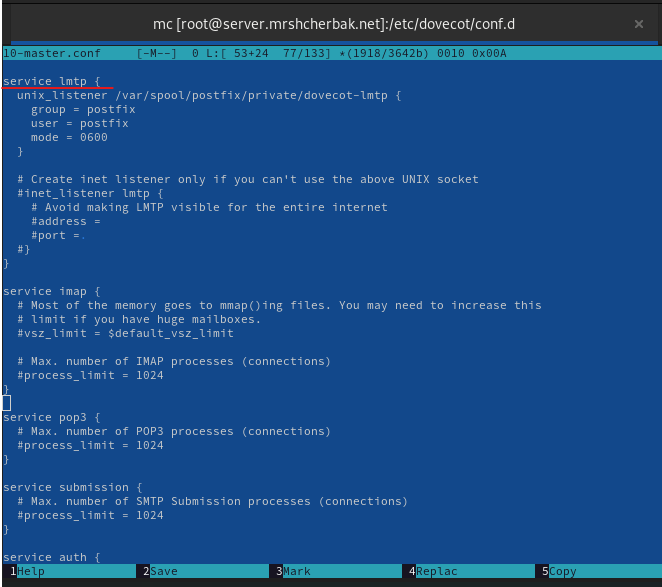


Рис.1.2. Настройка в Dovecot сервиса lmtp для связи с Postfix

4. Переопределила в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокет (рис.1.3).



Рис.1.3. Выполнение команды

5. В файле /etc/dovecot/conf.d/10-auth.conf задала формат имени пользователя для аутентификации в форме логина пользователя без указания домена (рис.1.4).

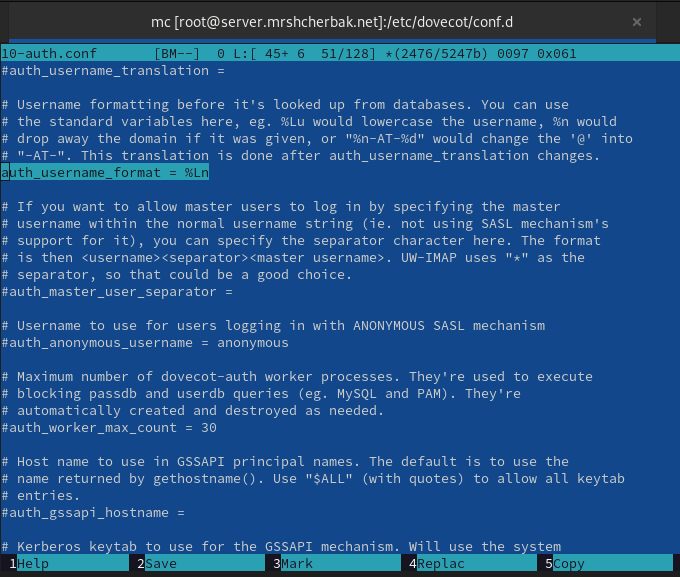


Рис.1.4. Редактирование файла /etc/dovecot/conf.d/10-auth.conf

6. Перезапустила Postfix и Dovecot (рис.1.5).



Рис.1.5. Выполнение команд

7. Из-под учётной записи своего пользователя отправила письмо с клиента (рис.1.6).



Рис.1.6. Отправка письма с клиента

Просмотрела логи при мониторинге почтовой службы (рис.1.6). Пользователь mrshcherbak устанавливает соединение с почтовым сервером через SMTP. Почтовый сервер принимает запрос от клиента mrshcherbak.net с IP-адресом 192.168.1.31, начинает обработку сообщения с идентификатором 20231203125459 от отправителя mrshcherbak. Сообщение добавляется в очередь для последующей обработки. Почтовый сервер закрывает соединение с клиентом после завершения этапа принятия данных. Dovecot, сервер для обработки входящей почты, устанавливает соединение для обработки сообщения. Dovecot получает и обрабатывает сообщение для пользователя mrshcherbak. Почтовый сервер передает сообщение Dovecot для доставки пользователю mrshcherbak через протокол IMAP. Успешное сохранение сообщения в почтовом ящике пользователя mrshcherbak. Удаление сообщения из очереди после успешной обработки.

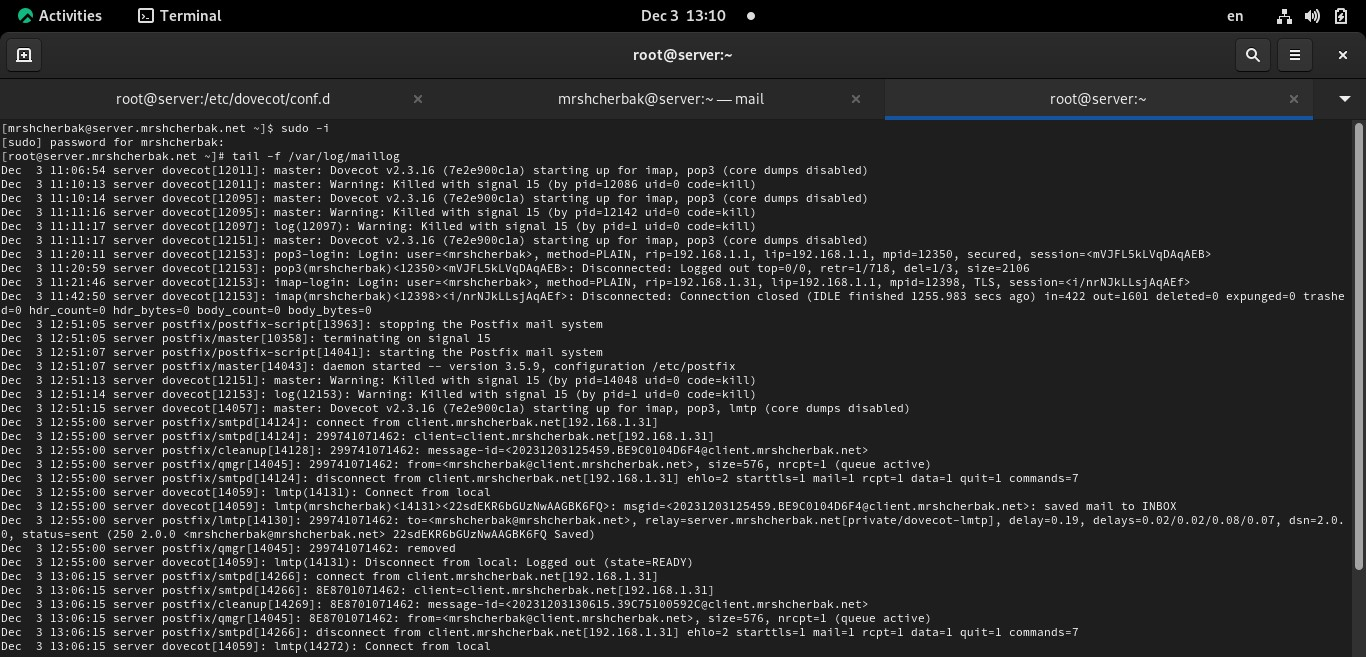


Рис.1.6. Мониторинг почтовой службы

Доставка сообщений в почтовый ящик (почтового клиента) (рис.1.7).

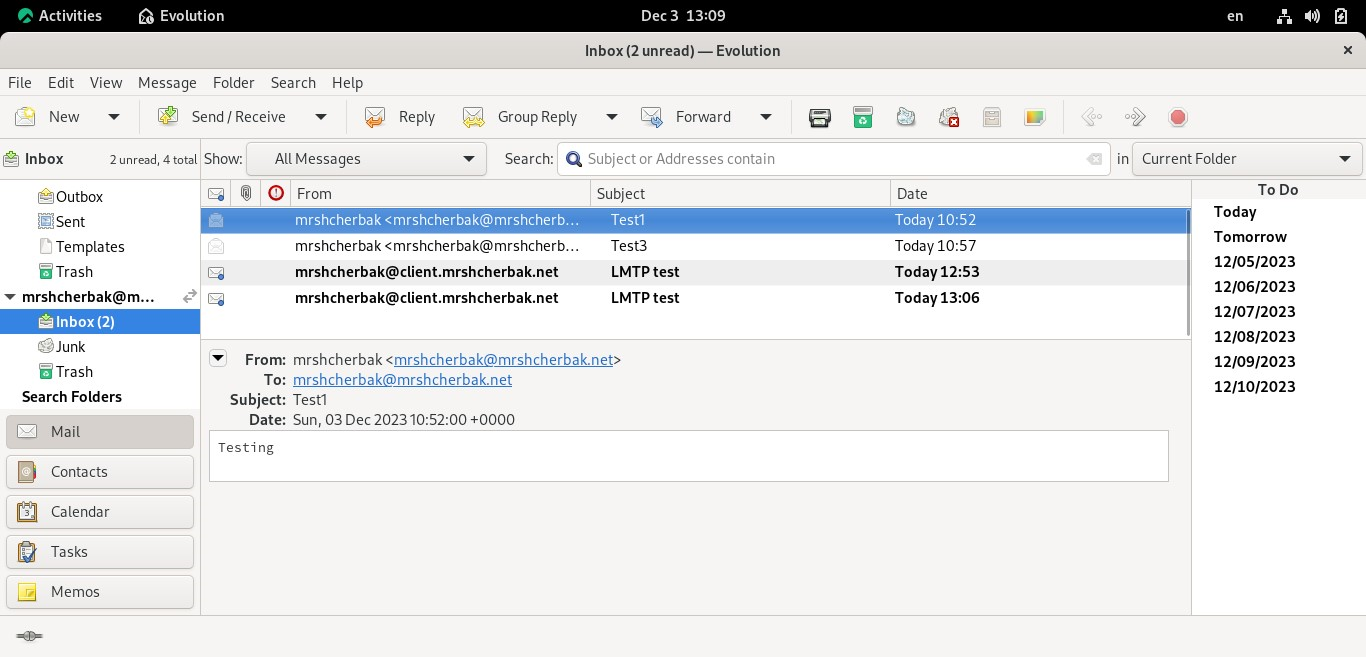


Рис.1.7. Проверка доставки писем

8. На сервере просмотрела почтовый ящик пользователя и убедилась, что отправленное с клиента письмо доставлено в почтовый ящик на сервере (рис.1.8).

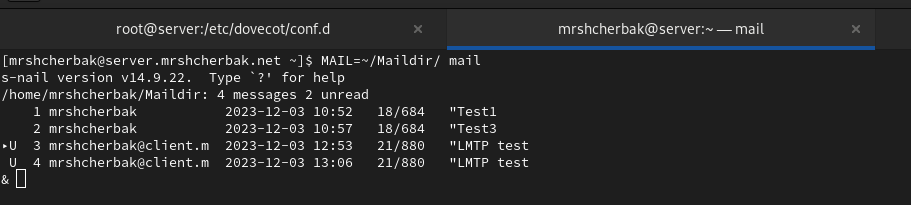


Рис.1.8. Проверка доставки писем

**2. Настройка SMTP-аутентификации**

1. В файле /etc/dovecot/conf.d/10-master.conf определила службу аутентификации пользователей (рис.2.1).

Фрагмент конфигурации в файле настраивает службу аутентификации пользователей.

service auth: начало блока конфигурации службы аутентификации.

Unix\_Listener /var/spool/postfix/private/auth : определение Unix сокета для службы аутентификации, используемого Postfix.

group = postfix: группа, к которой принадлежит сокет.

User = postfix: пользователь, которому принадлежит сокет.

mode = 0660: режим доступа к сокету.

unix\_listener auth-userdb: определение Unix сокета для процесса аутентификации пользователей.

mode = 0600: режим доступа к сокету аутентификации пользователей.

user = dovecot: пользователь, которому принадлежит сокет аутентификации пользователей.

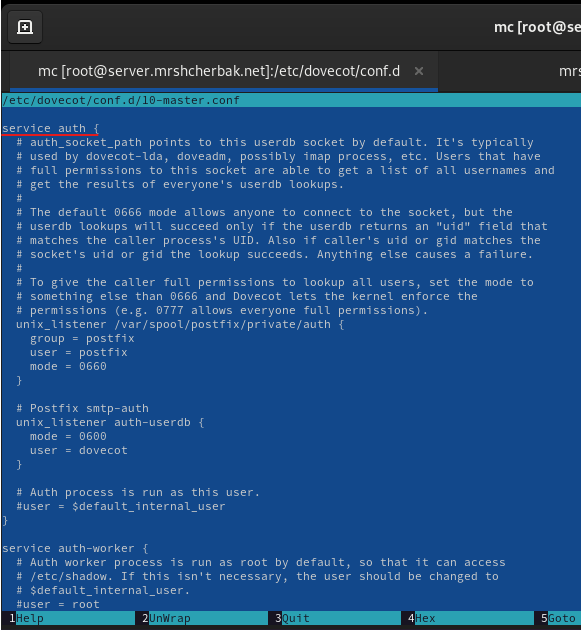


Рис.2.1. Содержимое файла /etc/dovecot/conf.d/10-master.conf

2. Для Postfix задала тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету, а также настроила Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины, обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок. В настройках Postfix ограничила приём почты только локальным адресом SMTP-сервера сети. Действия представлены на рис.2.2.

* postconf -e 'smtpd\_sasl\_type = dovecot': команда устанавливает тип аутентификации SASL для smtpd в значение "dovecot". Таким образом, Postfix будет использовать Dovecot для аутентификации пользователей.
* postconf -e 'smtpd\_sasl\_path = private/auth': устанавливает путь к unix-сокету для аутентификации SASL. Значение "private/auth" указывает на сокет, используемый Dovecot для аутентификации.
* postconf -e 'smtpd\_recipient\_restrictions = reject\_unknown\_recipient\_domain, permit\_mynetworks, reject\_non\_fqdn\_recipient, reject\_unauth\_destination, reject\_unverified\_recipient, permit': здесь настроены ограничения для приема почты. Каждый параметр разделенный запятой представляет собой различные правила:
* reject\_unknown\_recipient\_domain: отклоняет почту с неизвестным доменом получателя.
* permit\_mynetworks: разрешает отправку почты от клиентов в локальной сети, указанной в mynetworks.
* reject\_non\_fqdn\_recipient: отклоняет почту, если домен получателя не является полностью доменным именем.
* reject\_unauth\_destination: отклоняет почту с неподтвержденным адресом назначения.
* reject\_unverified\_recipient: отклоняет почту с неподтвержденным получателем.
* permit: разрешает все остальные случаи.
* postconf -e 'mynetworks = 127.0.0.0/8': команда определяет список сетей (mynetworks), которые считаются локальными. В данном случае, указана сеть 127.0.0.0/8, что включает в себя все IP-адреса в диапазоне от 127.0.0.1 до 127.255.255.255. Это позволяет ограничить прием почты только из локальной сети.

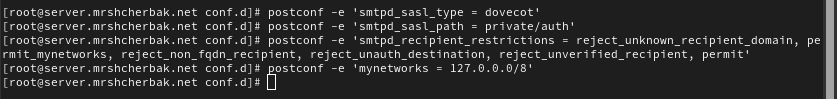


Рис.2.2. Выполнение команд

3. Для проверки работы аутентификации временно запустила SMTP-сервер (порт 25) с возможностью аутентификации. Для этого в файл /etc/postfix/master.cf внесла изменения (рис.2.3).

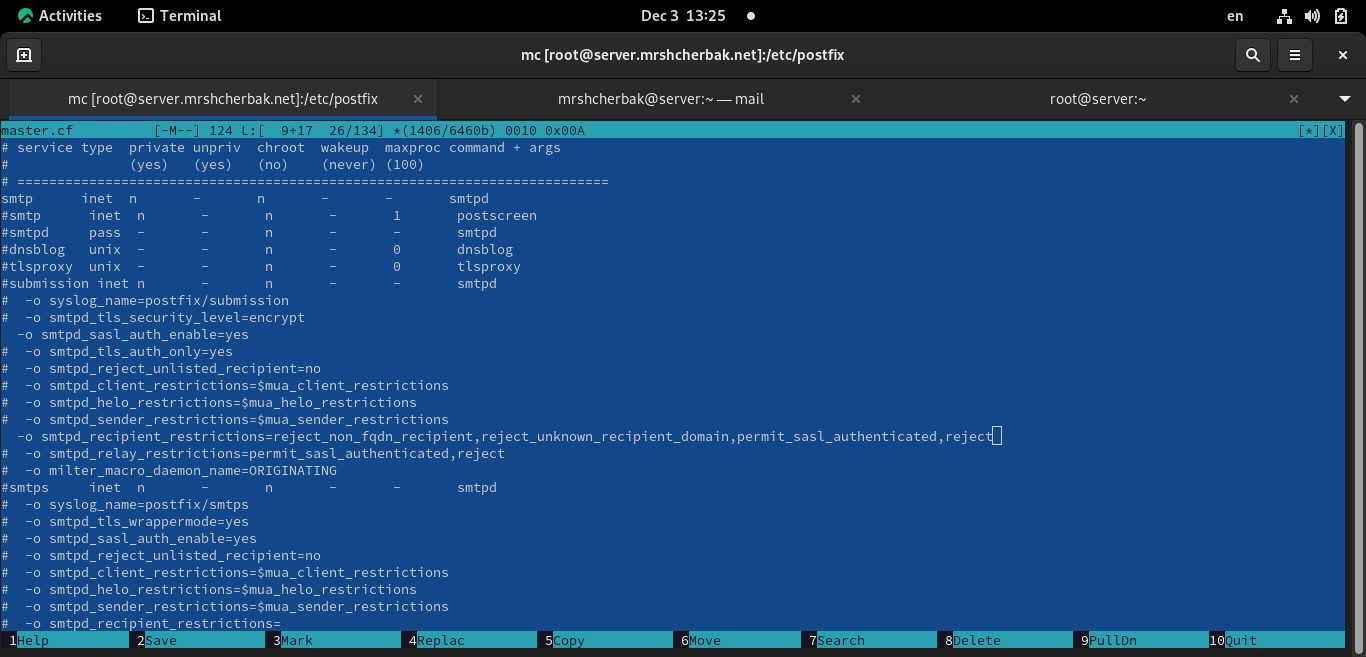


Рис.2.3. Редактирование файла /etc/postfix/master.cf

4. Перезапустила Postfix и Dovecot (рис.2.4).



Рис.2.4. Выполнение команд

5. На клиенте установила telnet (рис.2.5).

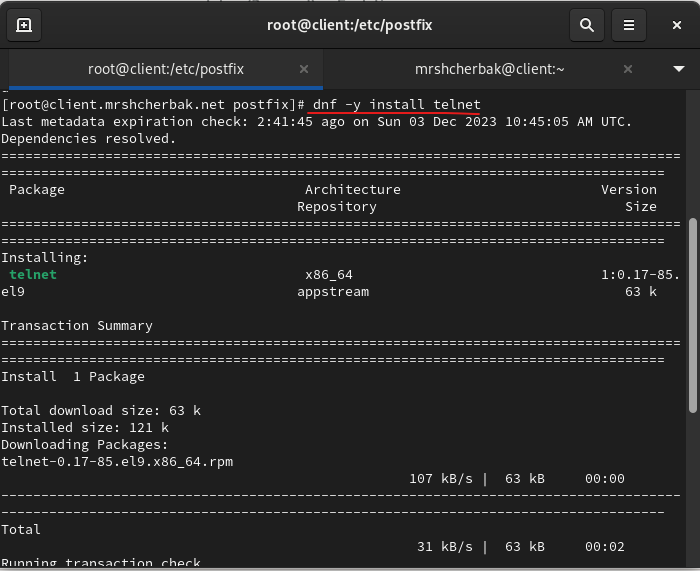


Рис.2.5. Установка telnet

6. На клиенте получила строку для аутентификации, подключилась к SMTP-серверу посредством telnet и протестировала соединение, введя EHLO test. Проверила авторизацию и завершила сессию. Действия представлены на рис.2.6.

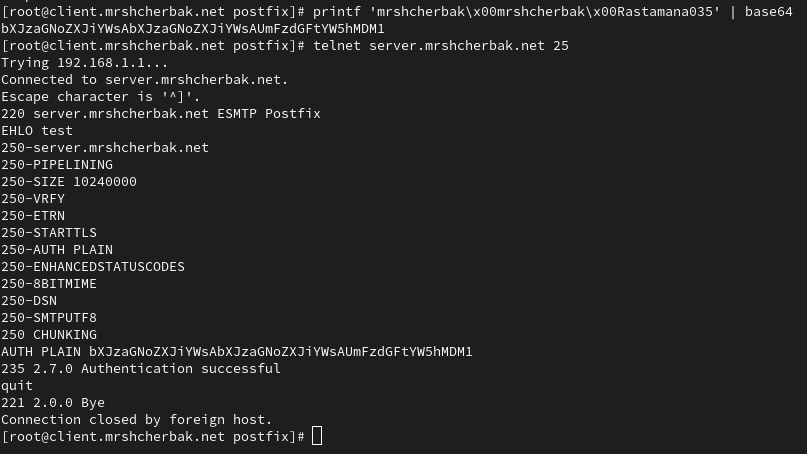


Рис.2.6. Выполнение команд

**3. Настройка SMTP over TLS**

1. Настроила на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно скопировала необходимые файлы сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги. Сконфигурировала Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности. Действия представлены на рис.3.1.

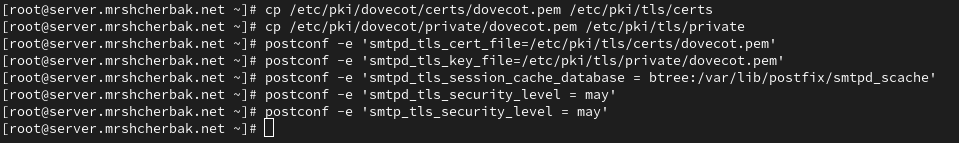


Рис.3.1. Выполнение команд

2. Для того чтобы запустить SMTP-сервер на 587-м порту, в файл /etc/postfix/master.cf внесла изменения (рис.3.2).



Рис.3.2. Редактирование файла /etc/postfix/master.cf

3. Настроила межсетевой экран, разрешив работать службе smtp-submission и перезапустила Postfix (рис.3.3).

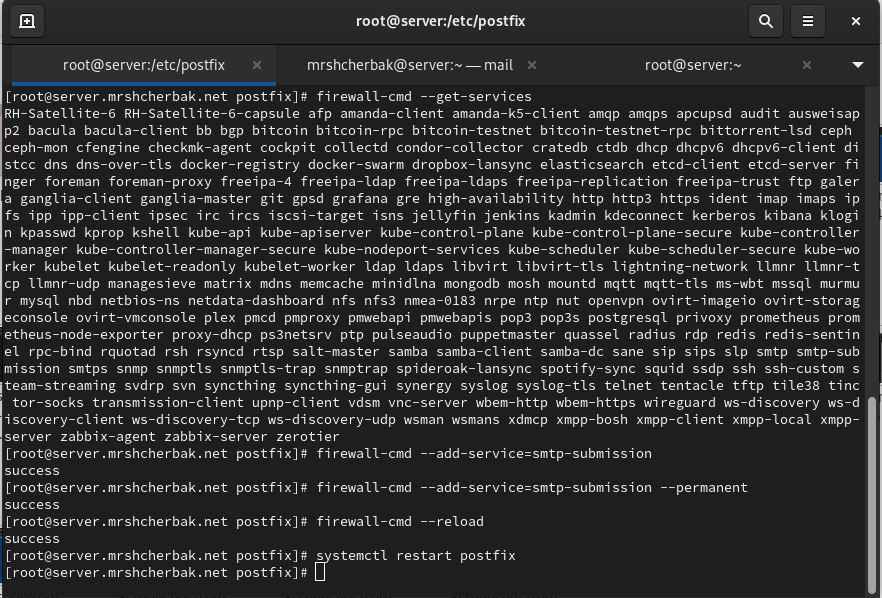


Рис.3.3. Выполнение команд

4. На клиенте подключилась к SMTP-серверу через 587-й порт посредством openssl и протестировала подключение по telnet, проверила аутентификацию (рис.3.4 – рис.3.6).

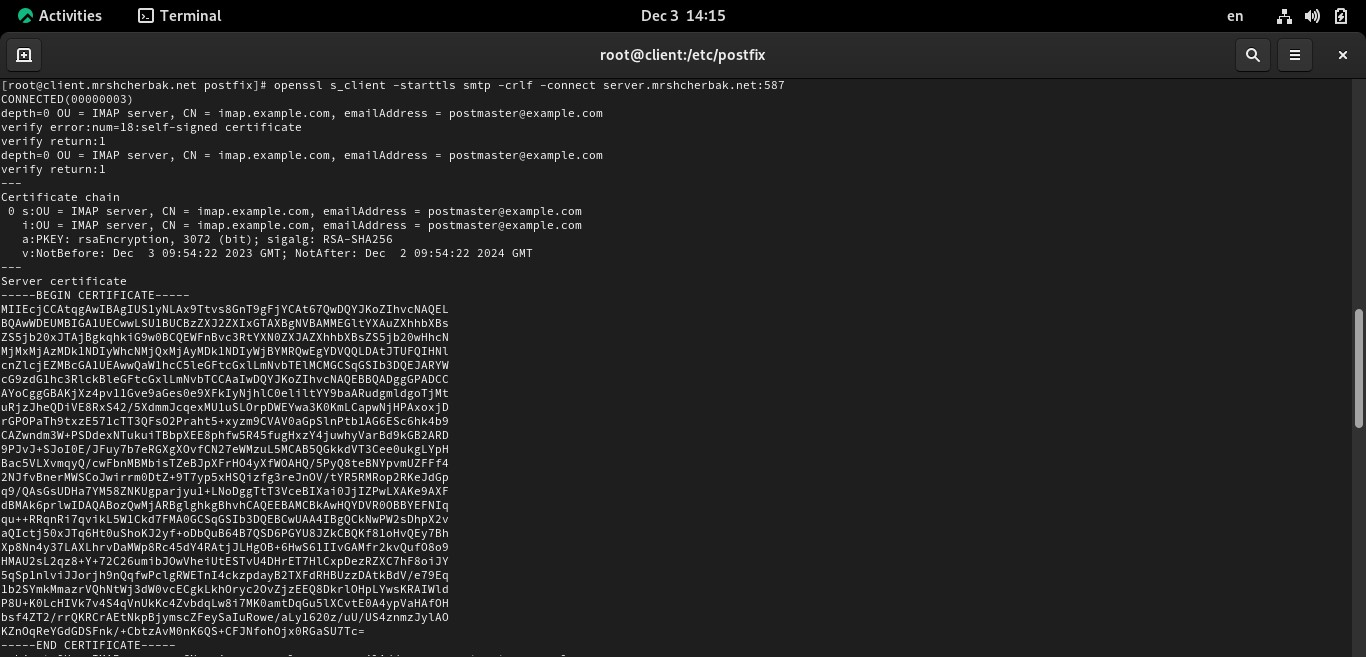


Рис.3.4. Подключение к SMTP-серверу через 587-й порт посредством openssl

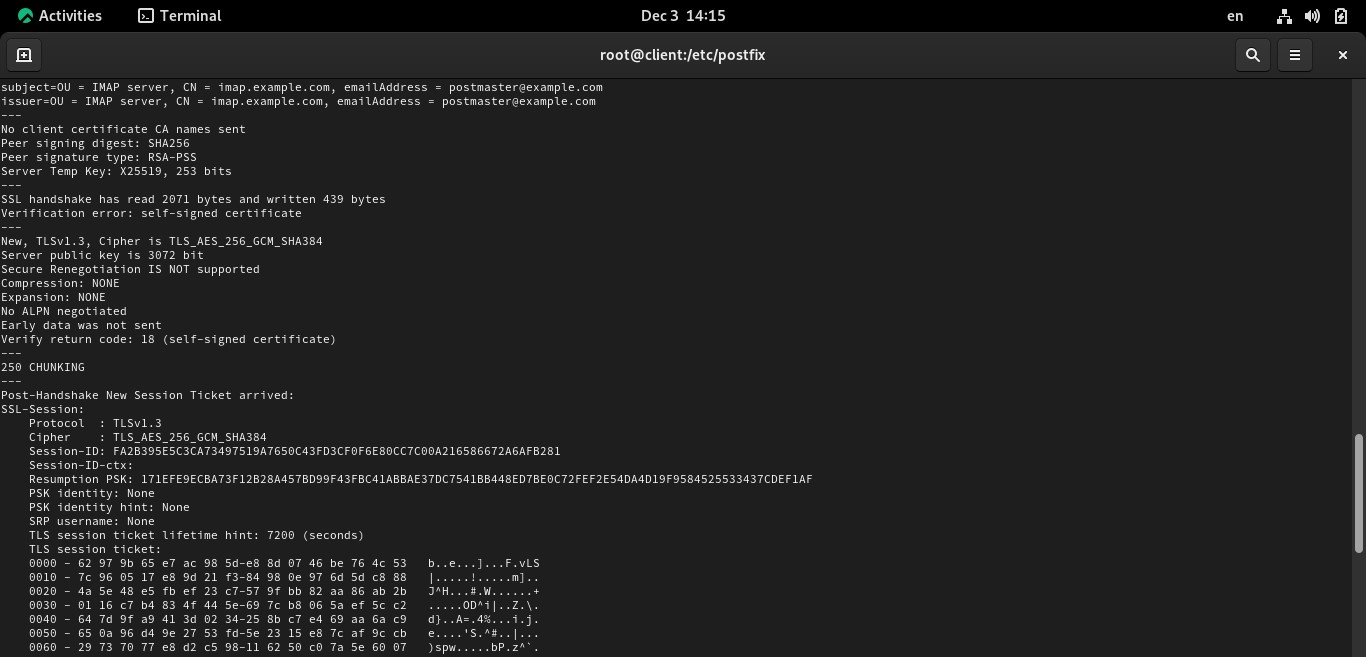


Рис.3.5. Подключение к SMTP-серверу через 587-й порт посредством openssl

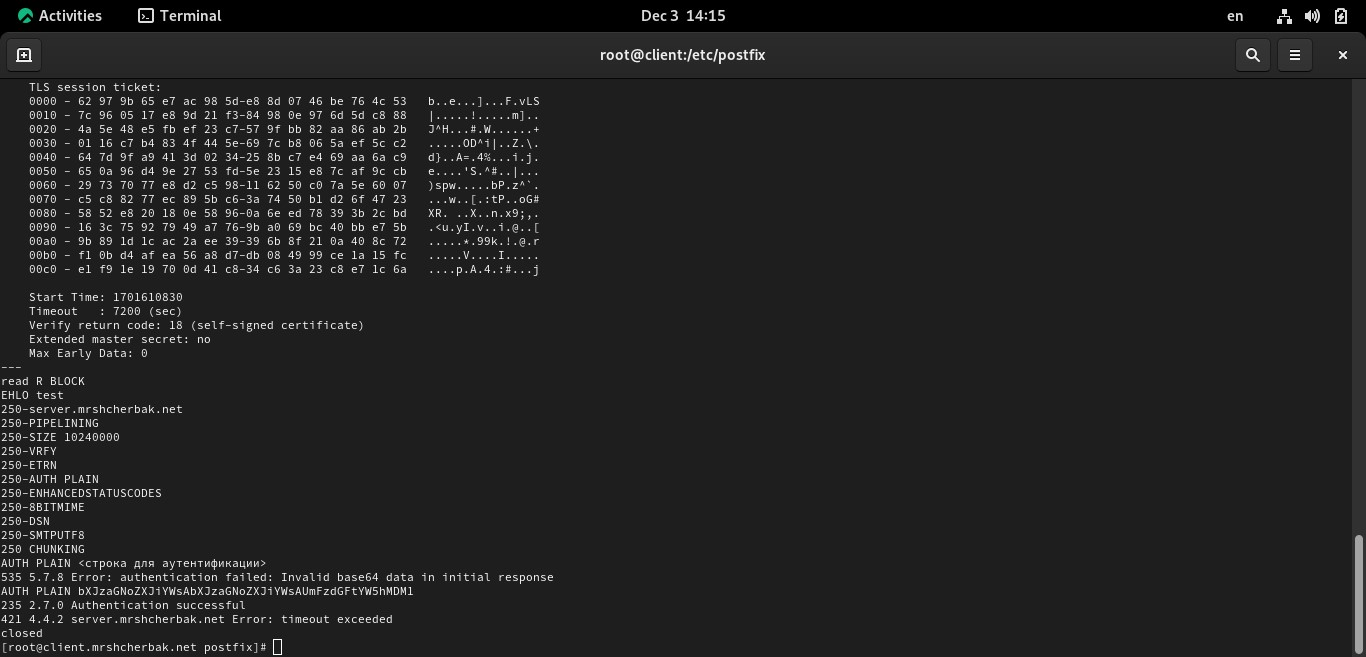


Рис.3.6. Тестирование подключения и проверка аутентификации

5. Проверила корректность отправки почтовых сообщений с клиента посредством почтового клиента Evolution, предварительно скорректировав настройки учётной записи, а именно для SMTP-сервера указала порт 587, STARTTLS и обычный пароль (рис.3.7 – рис.3.9).

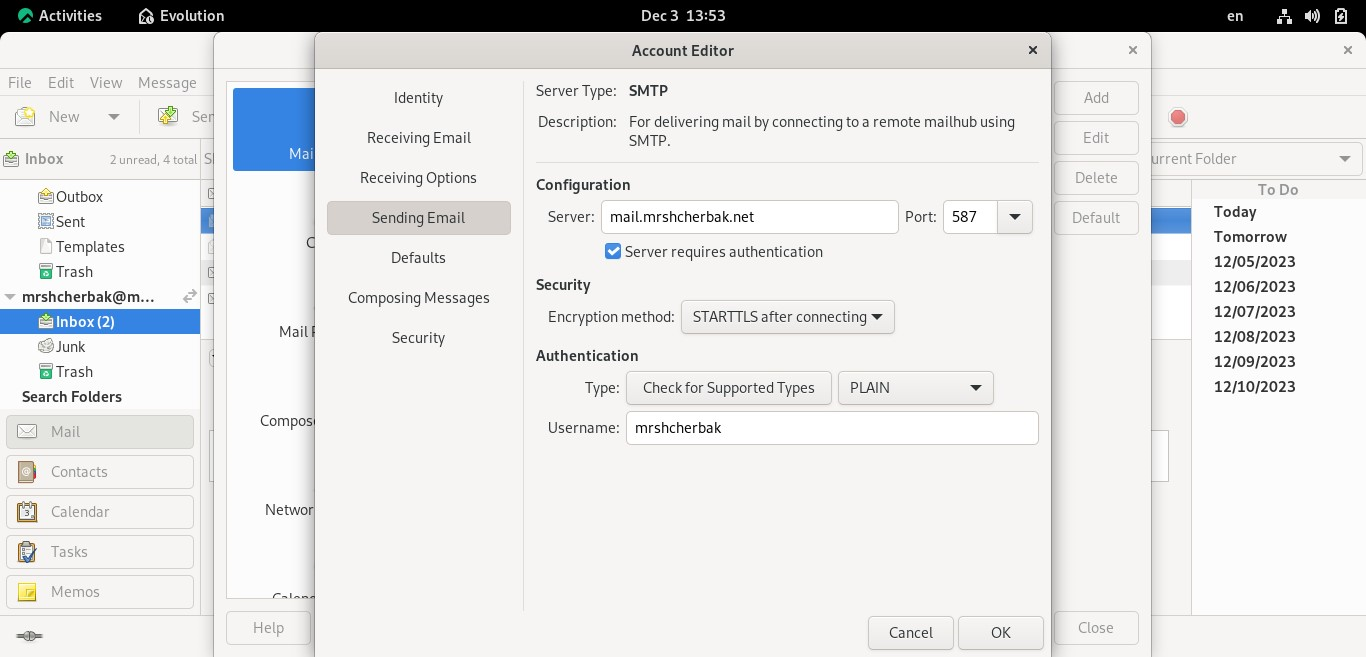


Рис.3.7. Настройка учетной записи

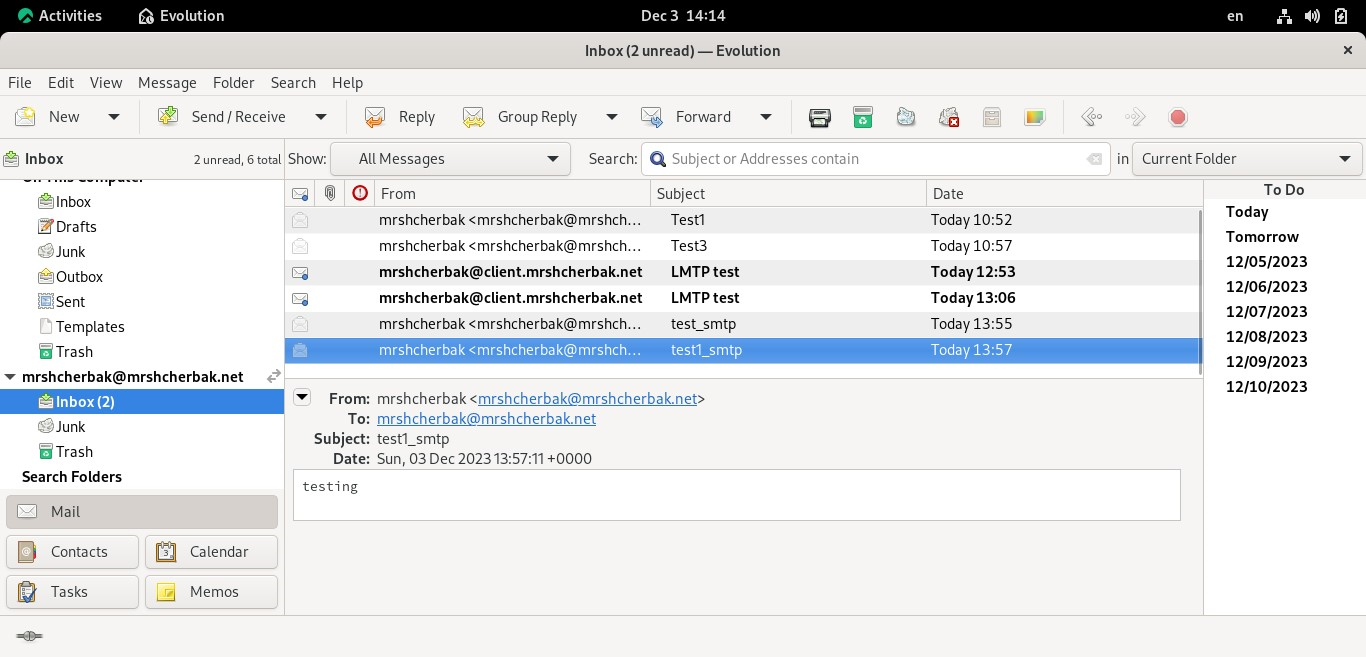


Рис.3.8. Проверка отправки почтовых сообщений с клиента

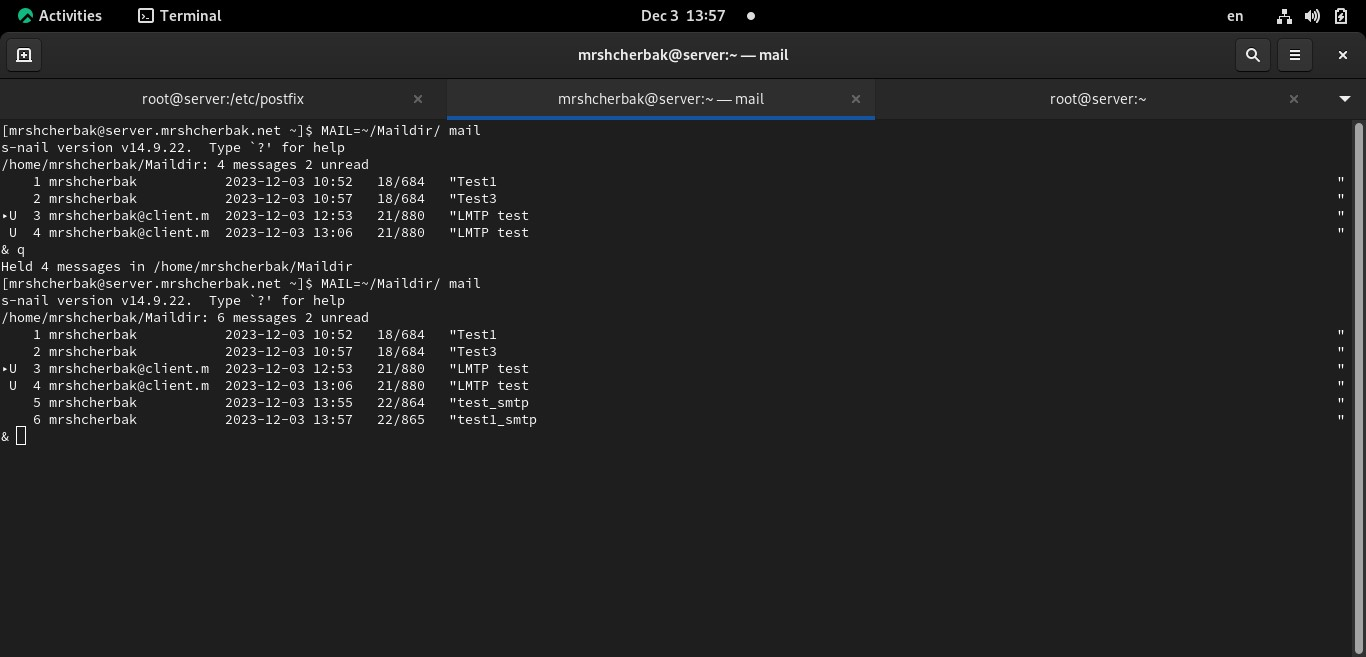


Рис.3.9. Проверка отправки почтовых сообщений с клиента

**4. Внесение изменений в настройки внутреннего окружения виртуальной машины**

1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/. В соответствующие подкаталоги поместила конфигурационные файлы Dovecot и Postfix (рис.4.1).

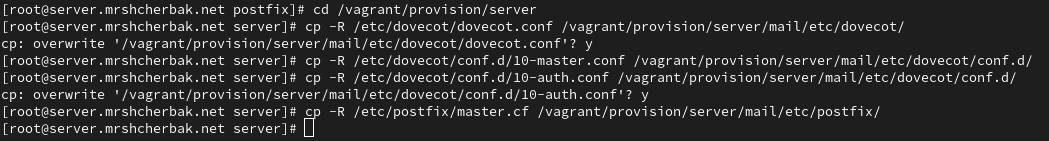


Рис.4.1. Выполнение команд

2. Внесла соответствующие изменения по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh (рис.4.2 – рис.4.3).

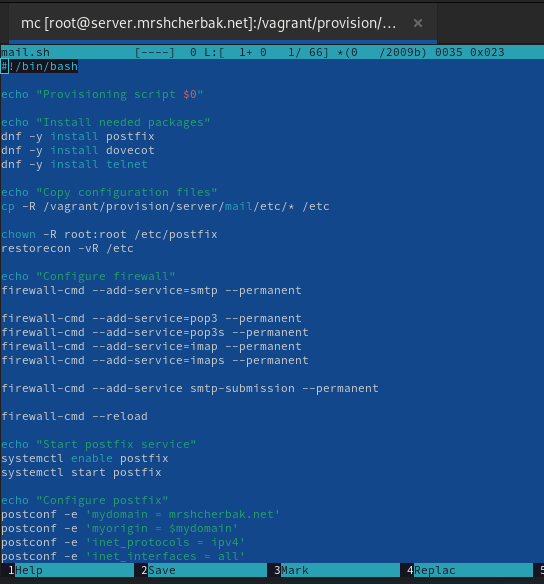


Рис.4.2. Содержимое файла /vagrant/provision/server/mail.sh

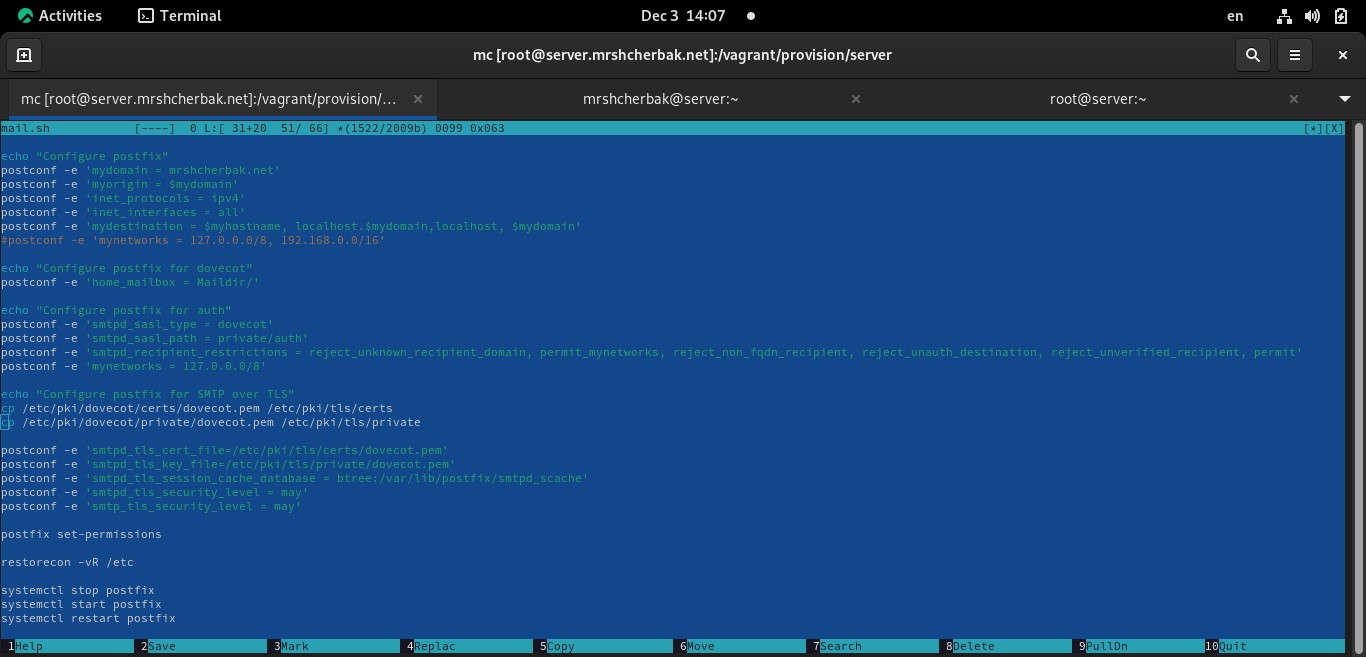


Рис.4.3. Содержимое файла /vagrant/provision/server/mail.sh

3. Внесла изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet (рис.4.4).

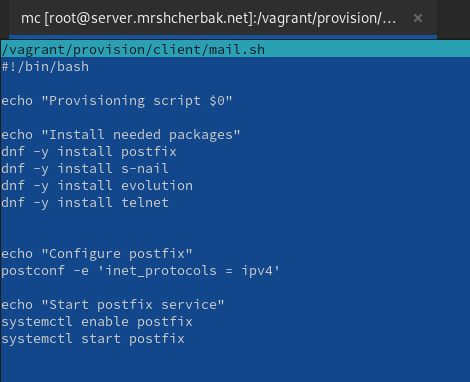


Рис.4.4. Содержимое файла /vagrant/provision/client/mail.sh

# Вывод: таким образом, в ходе выполнения л/р №10, я приобрела практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

# Контрольные вопросы

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

Пример: auth\_username\_format = %Ln@%Ld

В данном примере %Ln представляет логин пользователя, а %Ld представляет домен.

2. Какие функции выполняет почтовый Relay-сервер?

Почтовый Relay-сервер выполняет функцию передачи почты между различными почтовыми серверами. Он принимает почту от клиента и передает ее по маршруту доставки к почтовому серверу назначения. Это позволяет почтовым серверам в сети взаимодействовать и передавать сообщения между различными доменами.

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

Угрозы безопасности при настройке почтового сервера как Relay-сервера могут включать в себя:

* возможность использования сервера злоумышленниками для пересылки спама или злоупотребления ресурсами.
* злоумышленники могут использовать Relay-сервер для создания высокой нагрузки на сервер, что может привести к отказу в обслуживании (DoS) или снижению производительности.
* злоумышленники могут попытаться перехватить почту, передаваемую через Relay-сервер, для получения конфиденциальной информации.
* злоумышленники могут использовать Relay-сервер для массовой отправки спама. Это может привести к блокировке вашего сервера почтовыми сервисами и плохой репутации вашего IP-адреса.
* Злоумышленники могут использовать ваш сервер для отправки вредоносных вложений. Это может включать в себя различные виды вредоносных программ, вредоносных ссылок и т. д.
* Злоумышленники могут попытаться использовать ваш почтовый сервер в качестве прокси-сервера для скрытия своего местоположения и исходного IP-адреса при проведении вредоносных действий.

Для предотвращения этих угроз, необходимо правильно настраивать Relay-сервер, включая ограничение доступа и введение механизмов аутентификации.