Лабораторная работа №10

Расширенные настройки SMTP-сервера

Демидова Екатерина Алексеевна

Содержание

# 1 Цель работы

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

# 2 Задание

1. Настройте Dovecot для работы с LMTP.
2. Настройте аутентификацию посредством SASL на SMTP-сервере.
3. Настройте работу SMTP-сервера поверх TLS.
4. Скорректируйте скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server.

# 3 Выполнение лабораторной работы

## 3.1 Настройка LMTP в Dovecote

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом:

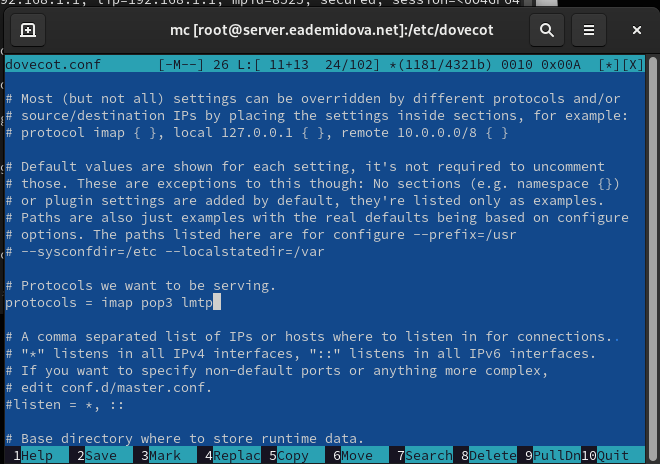
cd /var/tmp/eademidova/vagrant

Затем запустим виртуальную машину server:

make server-up

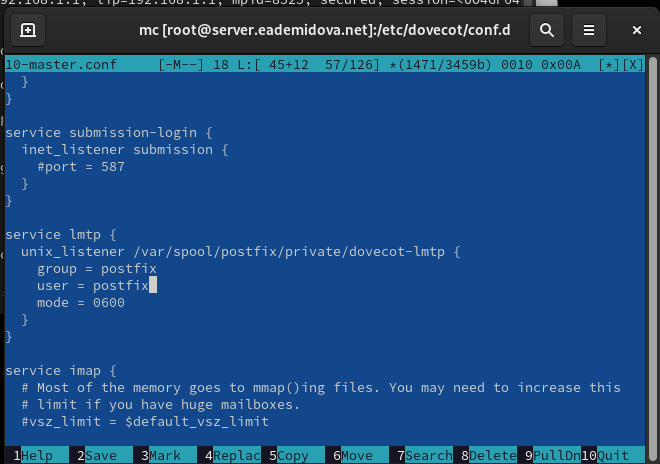
Откроем терминал и перейдем в режим суперпользователя

В дополнительном терминале запустим мониторинг работы почтовой службы с помощью команды tail -f /var/log/maillog. Затем добавим в список протоколов, с которыми модет работать Dovecot, протокол LMTP. Для этого в файле /etc/dovecot/dovecot.conf укажем(рис. ??):



Изменение списка протоколов для работы с Dovecot

Настроим в Dovecot сервис lmtp для связи с Postfix. Для этого в файле /etc/dovecot/conf.d/10-master.conf заменим определение сервиса lmtp на следующую запись(рис. ??):

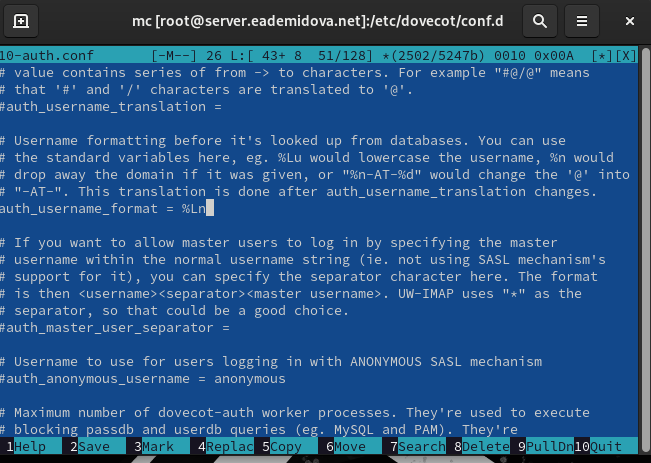


Настройка сервиса lmtp для связи с Postfix

Переопределим в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокет с помощью команды:

postconf -e 'mailbox\_transport = lmtp:unix:private/dovecot-lmtp'

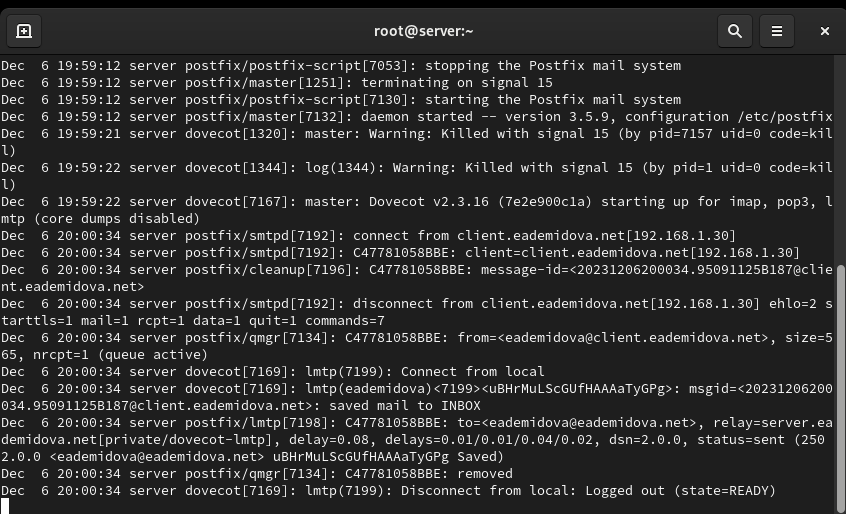
В файле /etc/dovecot/conf.d/10-auth.conf зададим формат имени пользователя для аутентификации в форме логина пользователя без указания домена:(??):



Задание формата имени пользователя

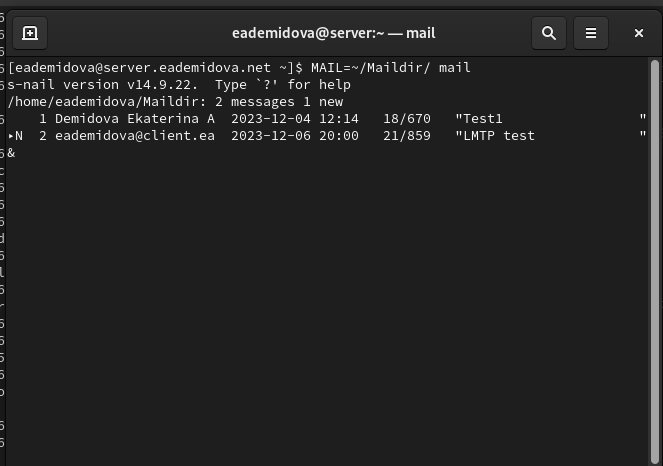
Затем перезапустим Postfix и Dovecot и из-под учетной записи своего пользователя отправим письмо с клиента.

Посмотрим информацию, которая вывелась при мониторинге почтовой службы(рис. ??):



Просмотр мониторинга почтовой службы

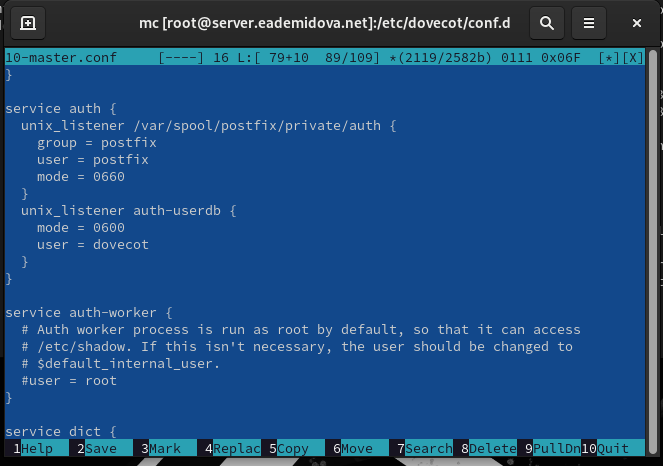
На сервере посмотрим почтовый ящик пользователя(??):



Просмотр почтового ящика пользователя

## 3.2 Настройка SMTP-аутентификации

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

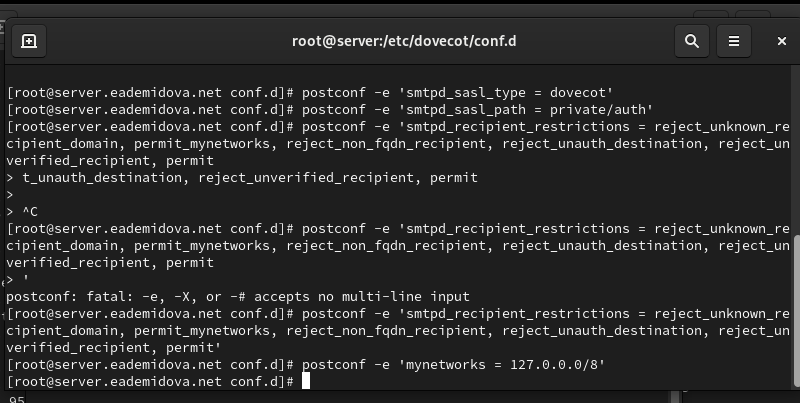


Определение службы аутентификации пользователей

В Postfix зададим каталог для доставки почты, затем сконфигурируем межсетевой экран, разрешив работать службам протоколов POP3 и IMAP, восстановим контекст безопасности SELinux, а затем перезапустим Postfix и запустим Dovecot

Мы указываем, что для аутентификации сервиса определена группа и пользователь postfix, задав права 0660 – владелец и группа могут читать и редактировать,остальные не имеют права выполнять никаких действий, и определен пользователь dovecot с правом 0600 – только владелец файла может читать/записывать.

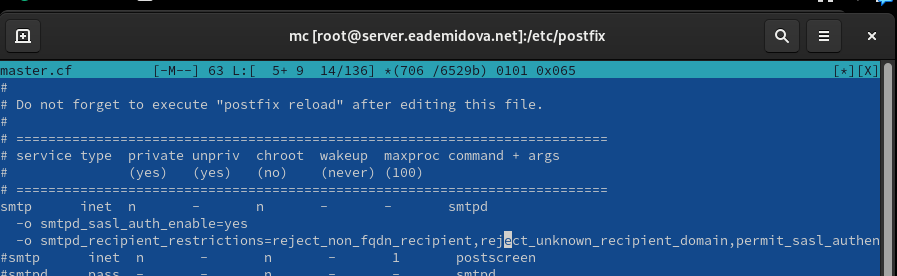
Для Postfix зададим тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету, затем настроим Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины(имеется в виду локальных пользователей сервера), обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок, а также в настройках Postfix ограничим приём почты только локальным адресом SMTP-сервера сети(??):



Конфигурации Postfix

* reject\_unknown\_recipient\_domain – отклонить запрос, если домен отправителя не имеет в DNS записей: MX и A
* permit\_mynetworks – разрешает все адреса, перечисленные в настройках mynetworks
* reject\_non\_fqdn\_recipient – отказать в соединении, если адрес получателя неверный
* reject\_unauth\_destination – запрещает подключение к службе без авторизации
* reject\_unverified\_recipient – отклонить запрос, если известно, что почта на адрес RCPT TO была отклонена или когда адрес получателя недоступен
* permit – Разрешить подключение. Присутствует в конце каждого блока (если письмо не попало не под одно правило запрета - доставляем)

Для проверки работы аутентификации временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Для этого изменим в файле /etc/postfix/master.cf(??):



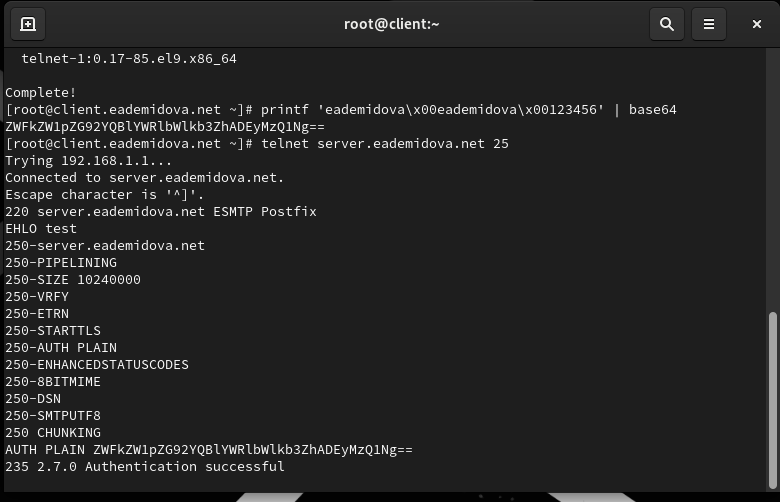
Временный запуск SMTP-сервера

Перезапустим Postfix и Dovecot

Теперь на клиенте установим telnet с помощью команд:

sudo -i  
dnf -y install telnet

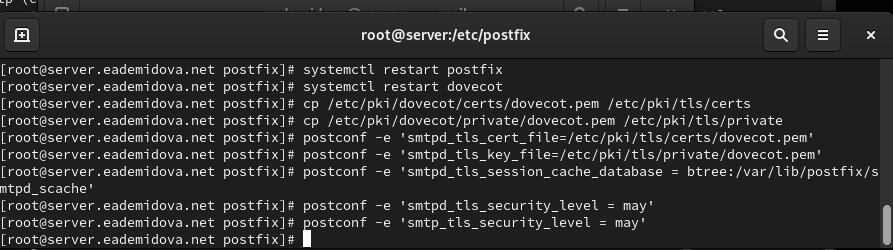
На клиенте получим строку для аутентификации и подключимся на клиенте к SMTP-серверу посредством telnet. Протестируем соединение и проверим авторизацию(??):



Получение строки для аутентификация и проверка посредством telnet

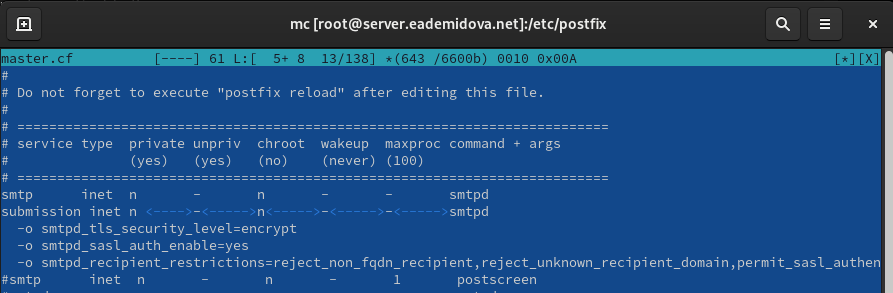
## 3.3 Настройка SMTP over TLS

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, затем сконфигурируем Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности(рис. ??):



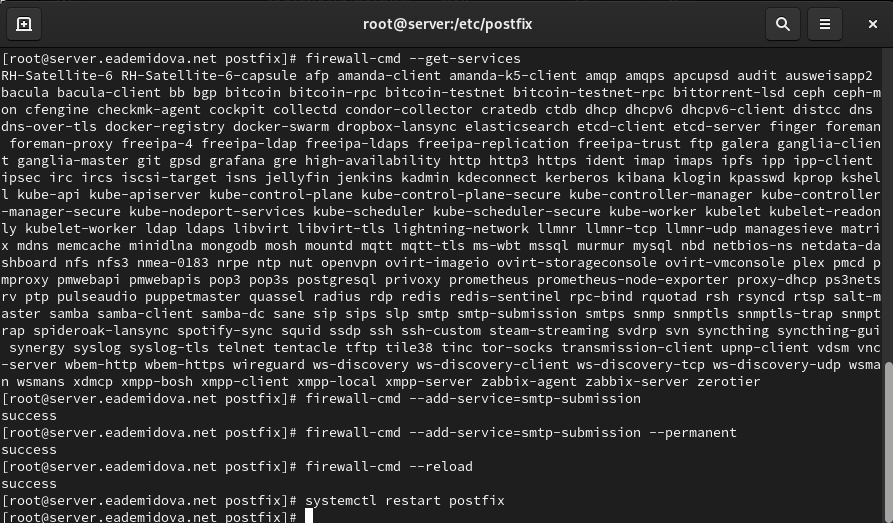
Конфигарции Postfix для настройки TLS

Для того чтобы запустить SMTP-сервер на 587-м порту, заменим содержимое файла /etc/postfix/master.cf(рис. ??):



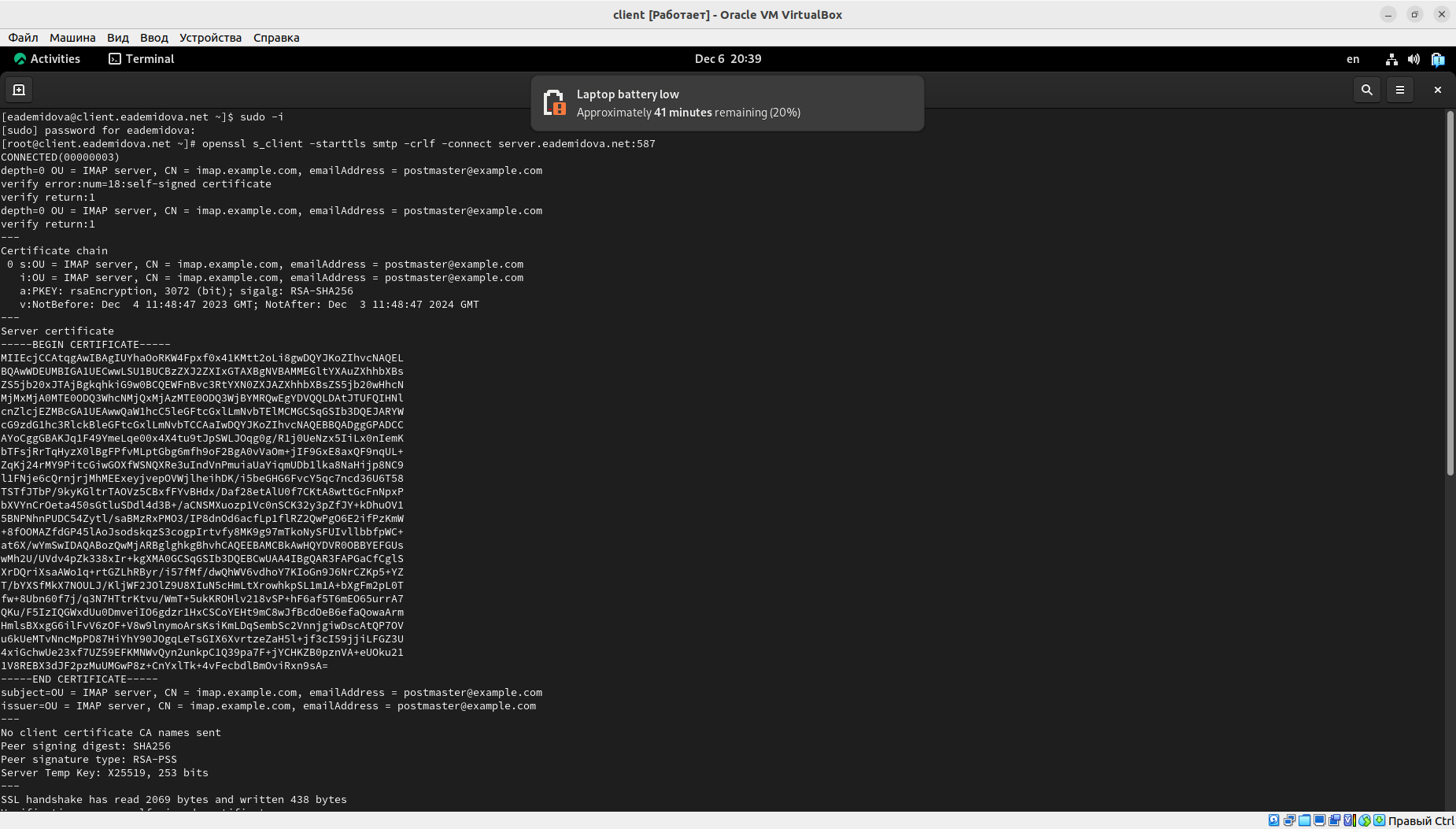
Изменение конфигураций для запуска SMTP-сервера на 587-порту

Настроим межсетевой экран, разрешив работать службе smtp-submission и перезапустим Postfix(??)



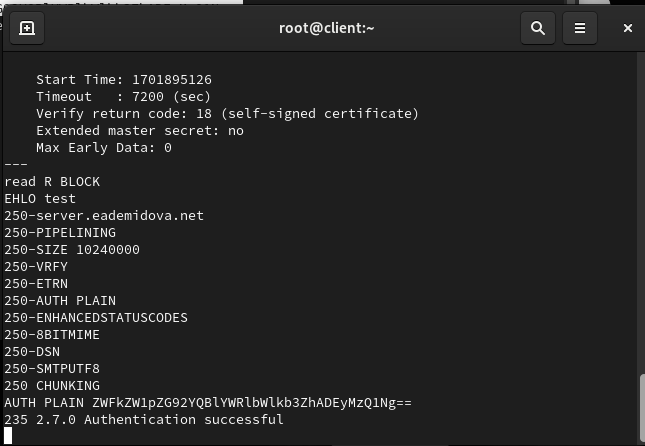
Настройка межсетевого экрана для работы службы smtp-submission

На клиенте подключитесь к SMTP-серверу через 587-й порт посредством openssl(рис. ??):



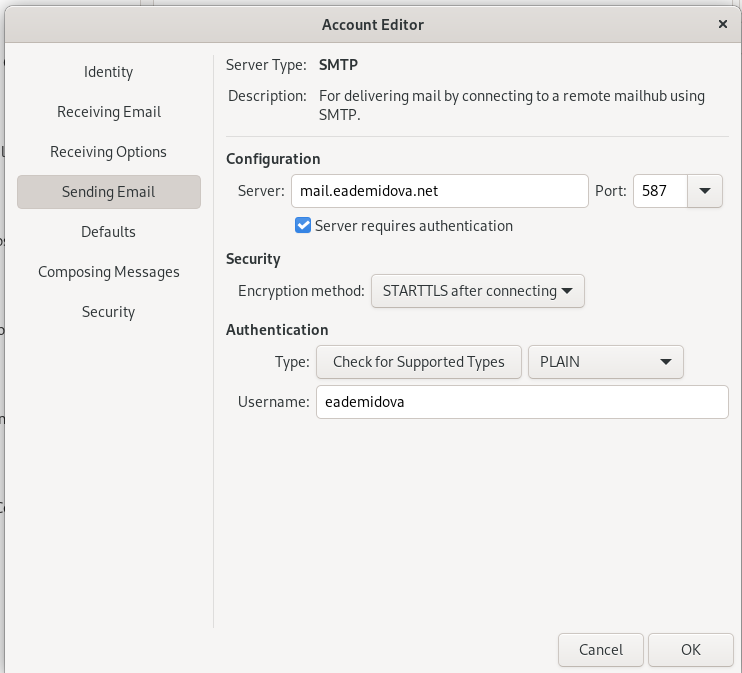
Подключение через openssl к SMTP-серверу

И протестируем подключение и аутентификацию по telnet(рис. ??):

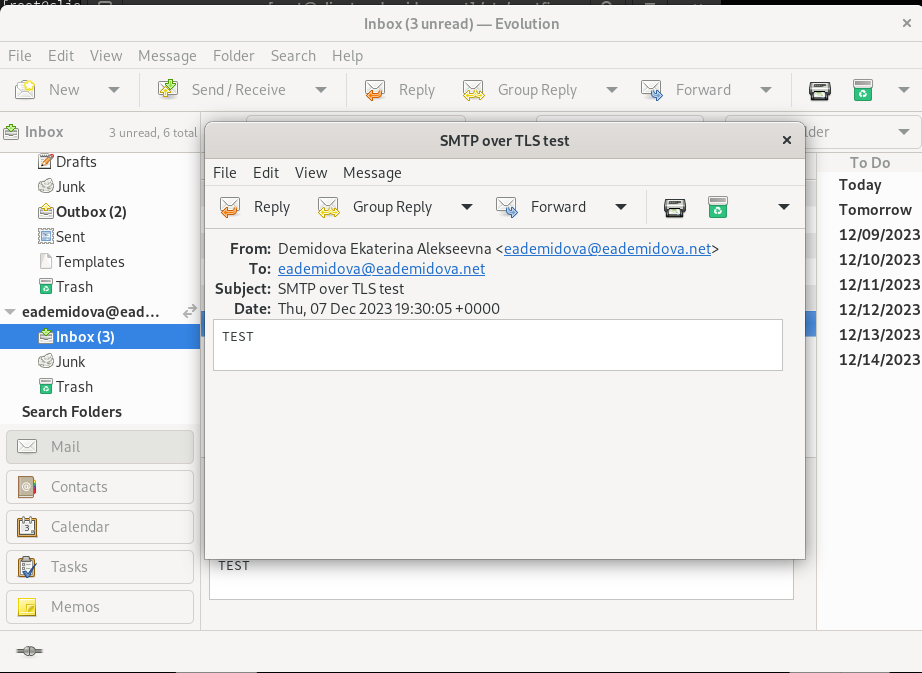


Проверка подключеня и аутентфикации по telnet

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(??, ??):



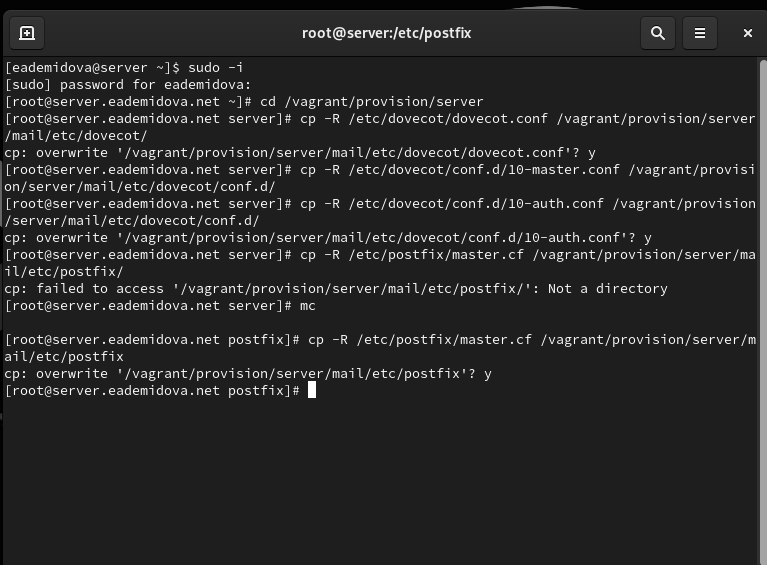
Изменение настроек учетной записи Evolution



Проверка корректности отправки почтовых сообщений с помощью Evolution

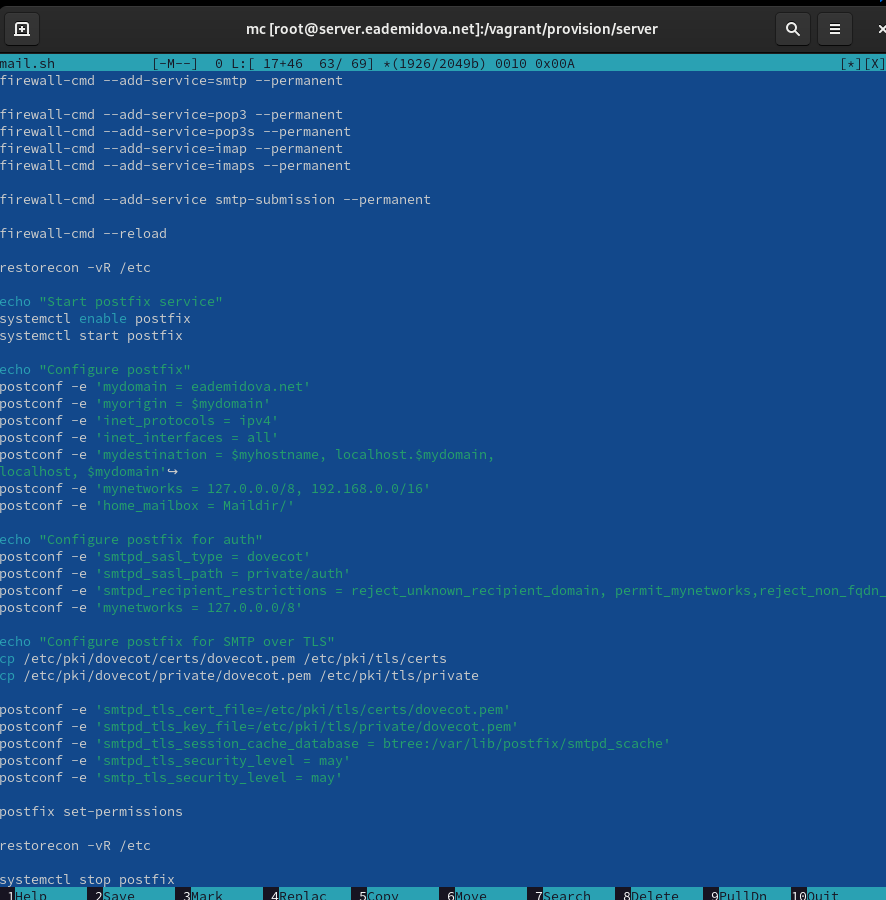
## 3.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

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



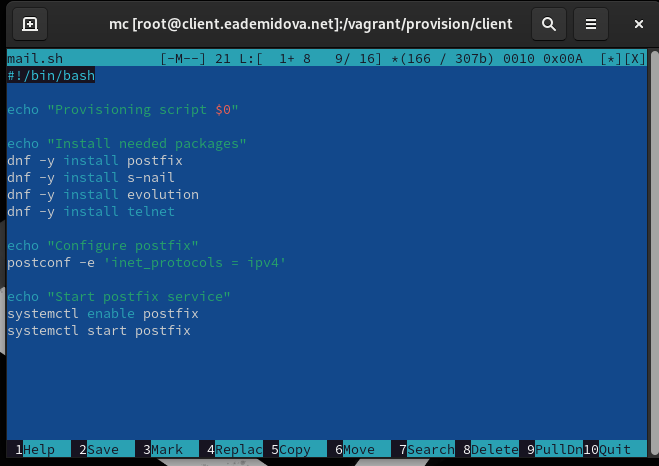
Создание окружения для внесения изменений в настройки окружающей среды

Внесем соответствующие изменения по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sht(??):



Изменение файла /vagrant/provision/server/mail.sh

На виртуальной машине client внесем изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet.(??):



Изменение файла /vagrant/provision/client/mail.sh

# 4 Контрольные вопросы

1. Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.
2. Какие функции выполняет почтовый Relay-сервер?
3. Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?
4. Пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена: auth\_username\_format = %Lu@%d
5. Почтовый Relay-сервер выполняет функции пересылки почты от одного почтового сервера к другому, облегчая маршрутизацию электронных сообщений между различными почтовыми системами.
6. Угрозы безопасности, связанные с настройкой почтового сервера как Relay-сервера, могут включать рассылку нежелательной почты (спам), перехват и изменение электронных сообщений, а также использование сервера для ретрансляции вредоносных сообщений.

# 5 Выводы

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