Отчёт по лабораторной работе 10

Расширенные настройки SMTP-сервера

Метвалли Ахмед Фарг Набеех

Содержание

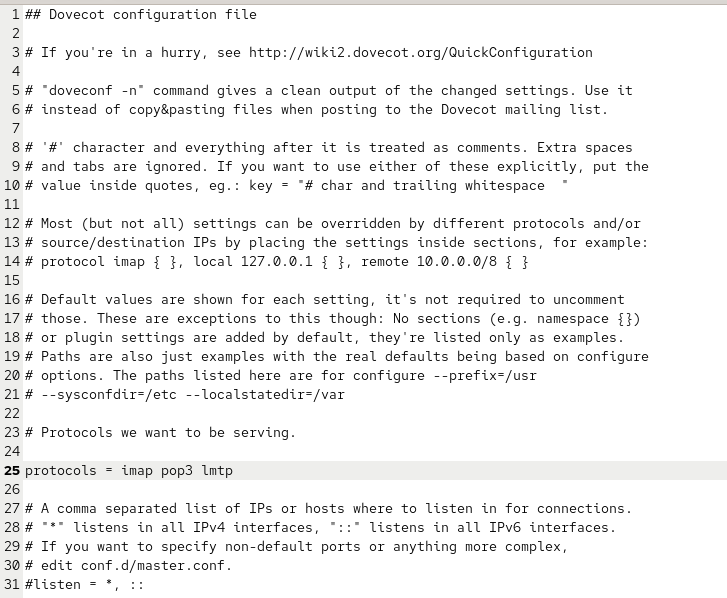
# 1 Цель работы

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

# 2 Выполнение

## 2.1 Настройка LMTP в Dovecot

1. На виртуальной машине server выполнен вход под собственным пользователем и выполнен переход в режим суперпользователя с помощью команды sudo -i.
2. В дополнительном терминале запущен мониторинг почтовой службы командой tail -f /var/log/maillog.
3. В файле /etc/dovecot/dovecot.conf добавлен протокол **LMTP** для поддержки локальной доставки почты.  
   В результате параметр **protocols** имеет вид:  
   protocols = imap pop3 lmtp

* 
* Рис. 1: Добавление LMTP в конфигурацию Dovecot

1. Для взаимодействия Dovecot с Postfix изменён блок service lmtp в файле /etc/dovecot/conf.d/10-master.conf.  
   Новый фрагмент конфигурации задаёт путь к Unix-сокету, права доступа и владельца:

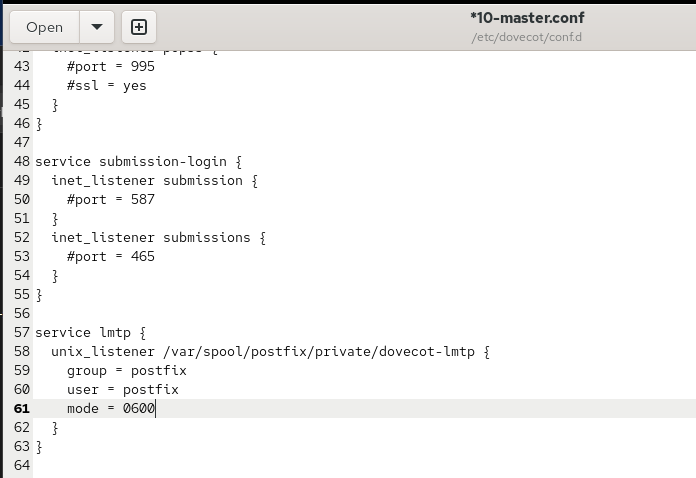


Рис. 2: Настройка сервиса lmtp в 10-master.conf

1. В файле /etc/dovecot/conf.d/10-auth.conf определён формат имени пользователя для аутентификации без доменной части:  
   auth\_username\_format = %Ln

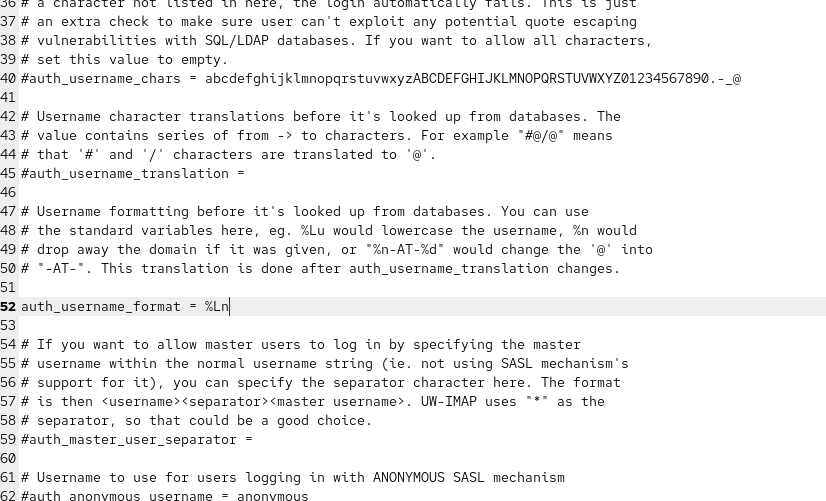


Рис. 3: Формат имени пользователя для аутентификации

1. В Postfix переопределена доставка сообщений через LMTP-сокет Dovecot:  
   postconf -e 'mailbox\_transport = lmtp:unix:private/dovecot-lmtp'
2. После изменения конфигурации службы **Postfix** и **Dovecot** были перезапущены:  
   systemctl restart postfix  
   systemctl restart dovecot
3. С клиентской машины отправлено тестовое письмо пользователю:  
   echo . | mail -s "LMTP test" ahmedfarg@ahmedfarg.net

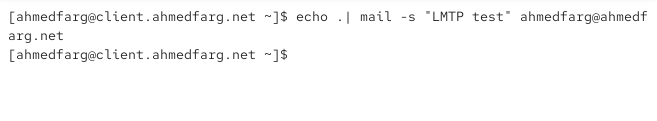


Рис. 4: Отправка тестового письма через LMTP

1. В логе почтовой службы зафиксирована успешная передача письма от Postfix к Dovecot по протоколу LMTP.  
   Видно, что сообщение сохранено в почтовом ящике пользователя.

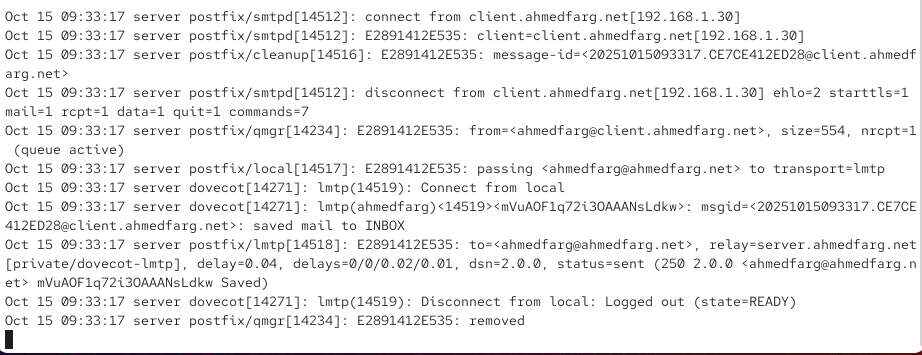


Рис. 5: Фрагмент лога доставки письма

1. На сервере проверено наличие доставленного письма в каталоге Maildir.  
   Сообщение с темой **“LMTP test”** присутствует в списке писем пользователя.

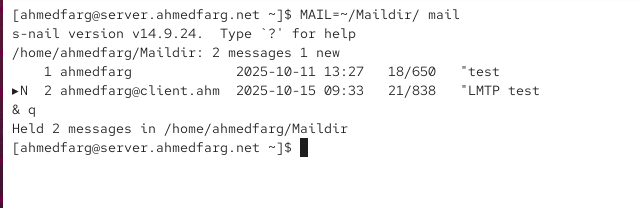
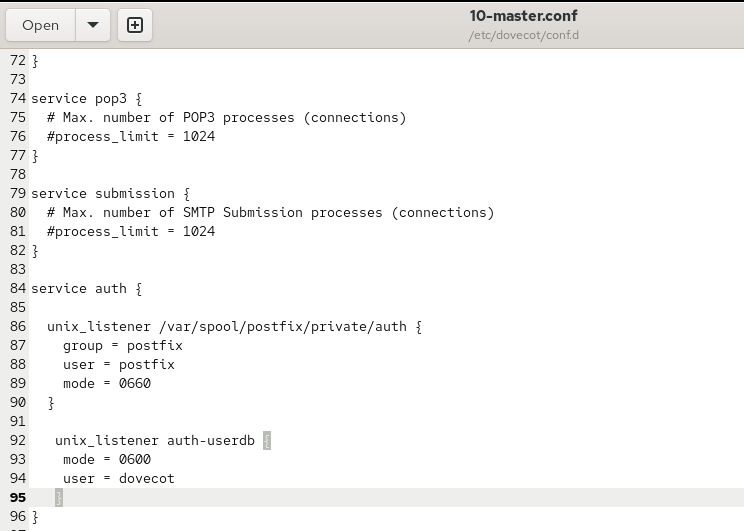


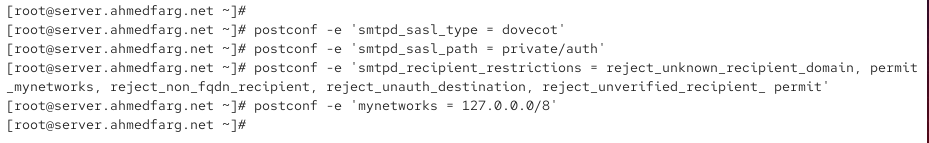
Рис. 6: Просмотр почтового ящика пользователя

## 2.2 Настройка SMTP-аутентификации

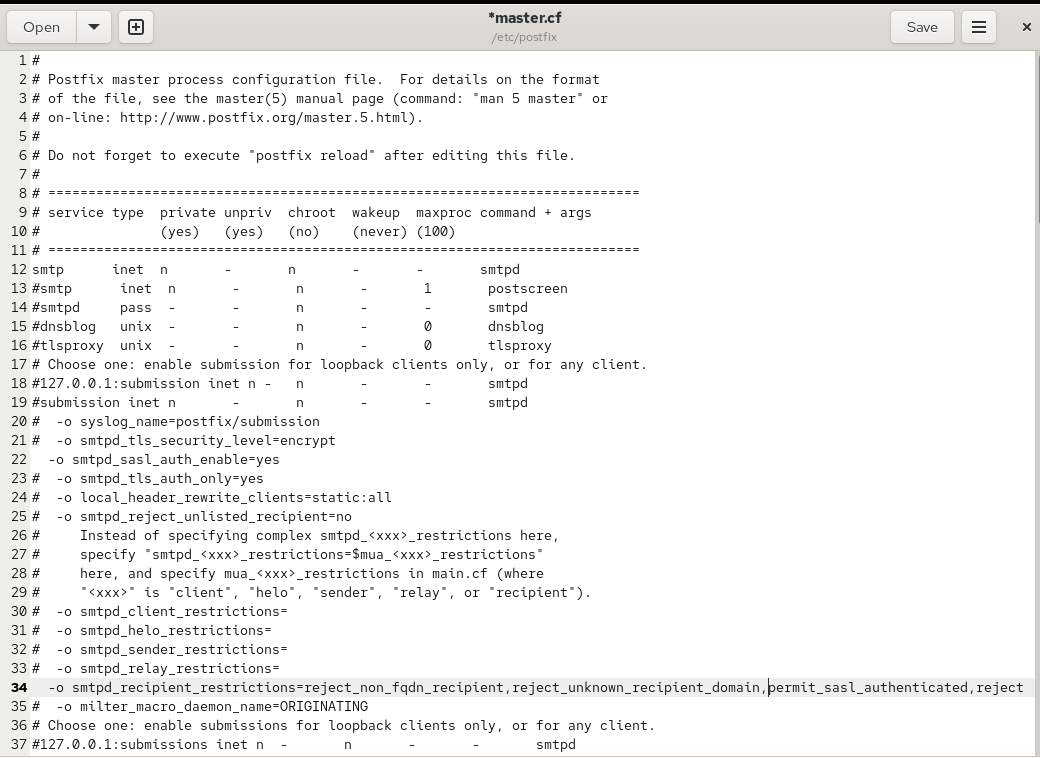
1. В файле /etc/dovecot/conf.d/10-master.conf определена служба аутентификации пользователей **auth**.  
   Этот блок конфигурации обеспечивает взаимодействие между Postfix и Dovecot через Unix-сокеты.

* **Пояснение:**  
  service auth — начало определения службы аутентификации Dovecot.  
  unix\_listener /var/spool/postfix/private/auth — создаёт Unix-сокет для связи Postfix с Dovecot.  
  group = postfix — задаёт группу владельца сокета.  
  user = postfix — определяет пользователя-владельца сокета.  
  mode = 0660 — разрешает чтение и запись для владельца и группы.  
  unix\_listener auth-userdb — внутренний сокет для взаимодействия Dovecot с базой данных аутентификации.  
  mode = 0600 — разрешение только для владельца.  
  user = dovecot — владелец внутреннего сокета — сервис Dovecot.
* 
* Рис. 7: Конфигурация сервиса аутентификации Dovecot

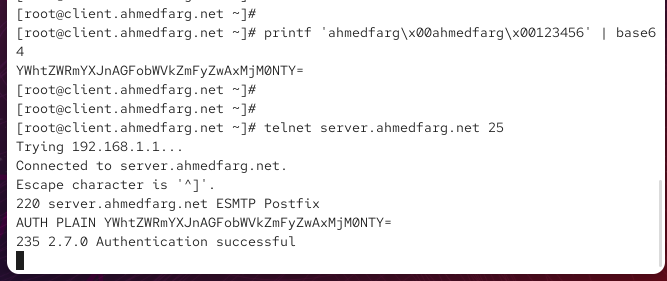
1. Для Postfix задан тип аутентификации SASL и путь к Unix-сокету, через который осуществляется проверка логинов.  
   Указано использование Dovecot в качестве механизма SASL и путь private/auth.

* 
* Рис. 8: Настройка SASL в Postfix

1. В Postfix настроены ограничения для приёма почты, предотвращающие использование сервера как открытого релея.  
   Опция smtpd\_recipient\_restrictions определяет последовательность проверок:
   * reject\_unknown\_recipient\_domain — отклоняет письма к несуществующим доменам.
   * permit\_mynetworks — разрешает приём писем от доверенных хостов.
   * reject\_non\_fqdn\_recipient — блокирует адреса без полного доменного имени.
   * reject\_unauth\_destination — запрещает пересылку на внешние домены.
   * reject\_unverified\_recipient — проверяет существование получателя.
   * permit — разрешает приём после успешного прохождения проверок.
2. Для ограничения доступа к серверу почтовые запросы разрешены только с локальной сети.  
   В параметре mynetworks задан диапазон 127.0.0.0/8.
3. В файле /etc/postfix/master.cf активирована возможность SMTP-аутентификации на порту 25.  
   В секции smtp inet добавлены параметры включения SASL-аутентификации и ограничений для проверки получателей.

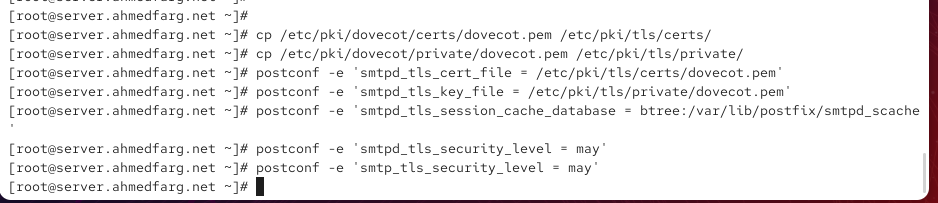
* 
* Рис. 9: Настройки аутентификации в master.cf

1. После внесённых изменений службы **Postfix** и **Dovecot** были перезапущены.
2. На клиенте установлена утилита **telnet** и сгенерирована строка для аутентификации в формате Base64.  
   Строка создаётся из логина и пароля пользователя в виде username username password.
3. С клиента выполнено подключение к SMTP-серверу по порту 25.  
   После ввода команды AUTH PLAIN <строка> сервер ответил сообщением  
   **235 2.7.0 Authentication successful**, что подтверждает успешную SMTP-аутентификацию.

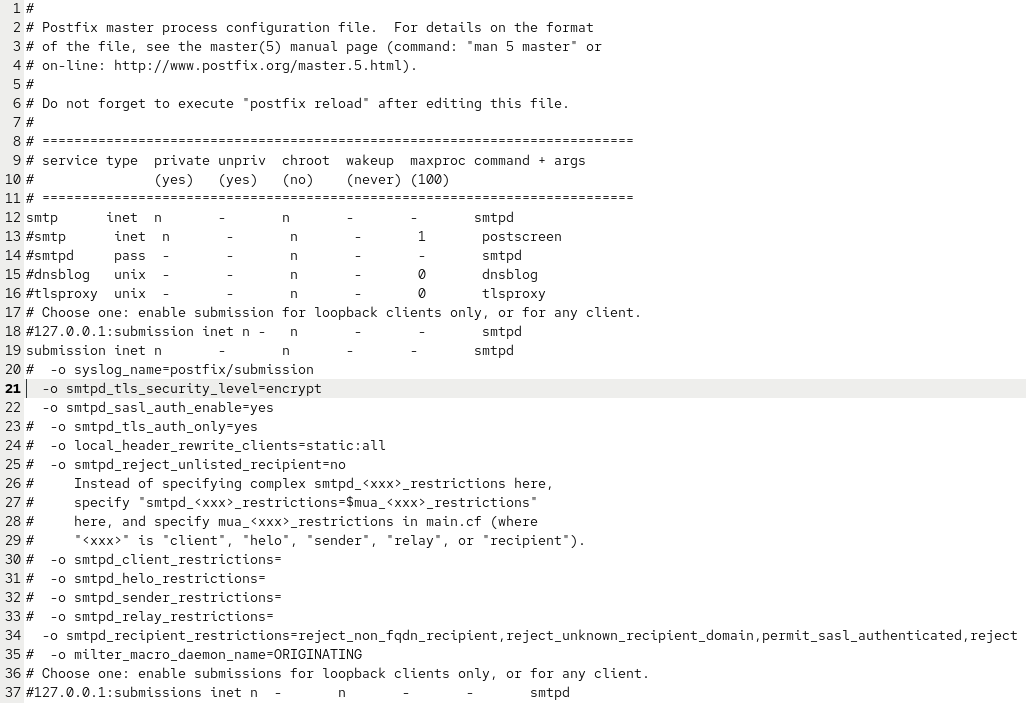
* 
* Рис. 10: Успешная SMTP-аутентификация через Telnet

## 2.3 Настройка SMTP over TLS

1. На сервере настроен TLS с использованием временного сертификата Dovecot.  
   Файлы сертификата и ключа скопированы из каталога /etc/pki/dovecot в /etc/pki/tls/ в соответствующие подкаталоги, чтобы избежать проблем с SELinux.  
   Далее в конфигурации Postfix указаны пути к файлам сертификата, ключа и каталогу для хранения TLS-сессий, а также определён уровень безопасности для шифрованных соединений.

* 
* Рис. 11: Настройка параметров TLS в Postfix

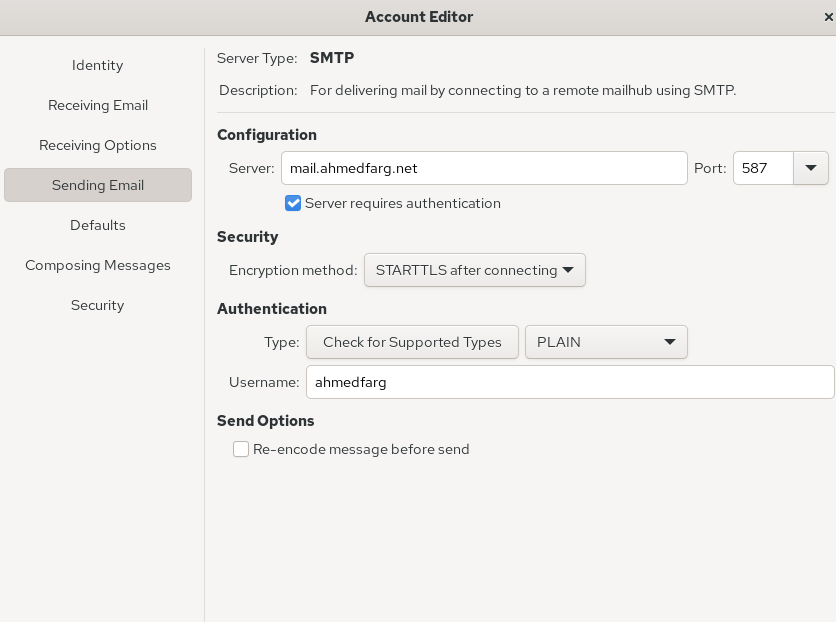
1. Для запуска SMTP-сервера на порту 587 в файле /etc/postfix/master.cf добавлена секция **submission**.  
   Она обеспечивает поддержку TLS и SASL-аутентификации, а также задаёт ограничения для проверки получателей.  
   Настройка секции выглядит следующим образом:
   * submission inet n - n - - smtpd — активация службы SMTP Submission.
   * -o smtpd\_tls\_security\_level=encrypt — обязательное шифрование соединений.
   * -o smtpd\_sasl\_auth\_enable=yes — включение аутентификации.
   * -o smtpd\_recipient\_restrictions=... — правила приёма сообщений.

* 
* Рис. 12: Добавление секции submission в master.cf

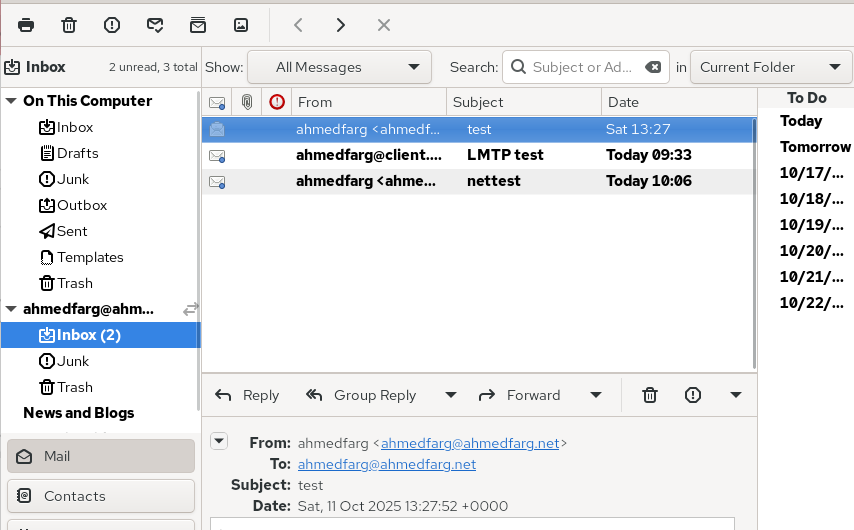
1. В межсетевом экране разрешена работа службы **smtp-submission**.  
   Это обеспечивает доступ к порту 587 как временно, так и на постоянной основе после перезапуска системы.
2. После внесения изменений служба **Postfix** была перезапущена для применения новых параметров конфигурации.
3. С клиентской машины выполнено подключение к SMTP-серверу через порт 587 с использованием openssl.  
   Проверка показала корректную работу TLS-соединения и успешную SMTP-аутентификацию пользователя.  
   Сервер ответил сообщением **235 2.7.0 Authentication successful**, что подтверждает защищённое подключение и успешную проверку учётных данных.

* 
* Рис. 13: Проверка TLS-подключения и успешная аутентификация

1. В почтовом клиенте **Evolution** внесены изменения в настройки отправки почты.  
   Для SMTP-сервера указан порт **587**, метод шифрования **STARTTLS after connecting** и тип аутентификации **PLAIN**.  
   Пользователь вводит логин для проверки подлинности при отправке писем.

* 
* Рис. 14: Настройка SMTP с STARTTLS в почтовом клиенте

1. Отправка почтовых сообщений с клиента успешно проверена.  
   Входящие письма отображаются в папке **Inbox**, что подтверждает корректную работу SMTP over TLS и шифрованную доставку сообщений.

* 
* Рис. 15: Проверка доставки почты через TLS

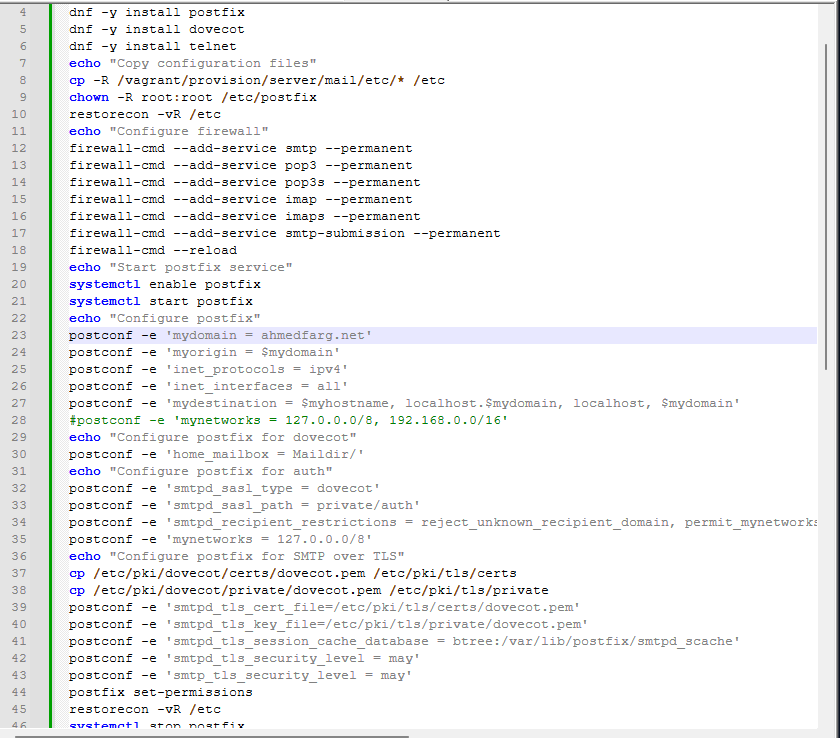
# 3 Выполнение

## 3.1 Внесение изменений в настройки внутреннего окружения виртуальной машины

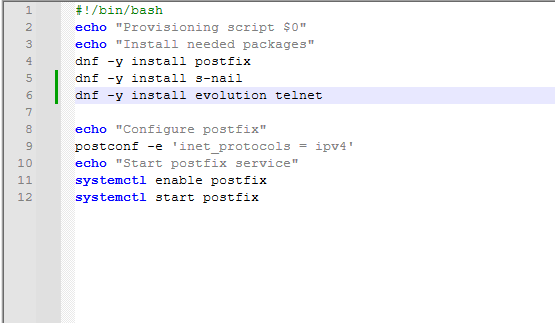
1. На виртуальной машине server выполнен переход в каталог /vagrant/provision/server/ для внесения изменений в настройки окружения.  
   В соответствующие подкаталоги помещены конфигурационные файлы **Dovecot** и **Postfix**.

* 
* Рис. 16: Копирование конфигурационных файлов Dovecot и Postfix

1. В файл /vagrant/provision/server/mail.sh внесены изменения для расширенной конфигурации SMTP-сервера.

* 
* Рис. 17: Обновлённый скрипт конфигурации сервера mail.sh

1. В файл /vagrant/provision/client/mail.sh добавлена установка пакета telnet и почтового клиента evolution, необходимых для тестирования и проверки работы SMTP-сервера.

* 
* Рис. 18: Изменённый скрипт клиента mail.sh

# 4 Заключение

SMTP-сервер был успешно настроен для работы с безопасной аутентификацией и шифрованием с использованием TLS.  
Dovecot и Postfix интегрированы через LMTP и SASL, что обеспечивает корректную доставку и защищённую передачу почты.

# 5 Контрольные вопросы

1. **Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.**  
   Формат указывается в параметре auth\_username\_format, например:  
   auth\_username\_format = %n@%d  
   где %n — имя пользователя, а %d — домен (например, user@example.com).
2. **Какие функции выполняет почтовый Relay-сервер?**  
   Relay-сервер (посредник) принимает почту от одного почтового узла и пересылает её другому серверу, выступая промежуточным звеном между отправителем и конечным получателем.  
   Основные функции — маршрутизация сообщений, передача писем между доменами и поддержка внешних соединений при отправке почты.
3. **Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?**  
   Если почтовый сервер настроен как открытый релей (Open Relay), он может быть использован злоумышленниками для рассылки спама и фишинговых писем.  
   Это приведёт к блокировке IP-адреса сервера, попаданию в «чёрные списки» и снижению доверия к почтовому домену.  
   Также возможно увеличение нагрузки и утечка конфиденциальных данных при отсутствии аутентификации и шифрования.