РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 10

**Расширенные настройки SMTP-сервера**

*дисциплина: Администрирование* *Сетевых Подсистем*

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

**Цель работы:**

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

**Выполнение работы:**

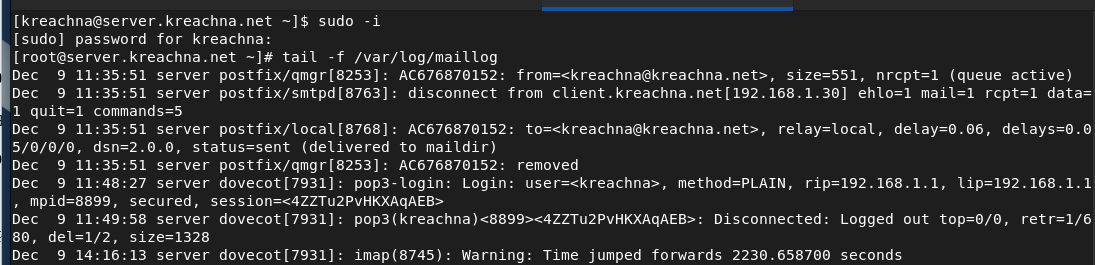
1. **Настройка LMTP в Dovecote**
2. На виртуальной машине server войдите под вашим пользователем и откройте терминал. Перейдите в режим суперпользователя:

sudo -i

1. В дополнительном терминале запустите мониторинг работы почтовой службы:

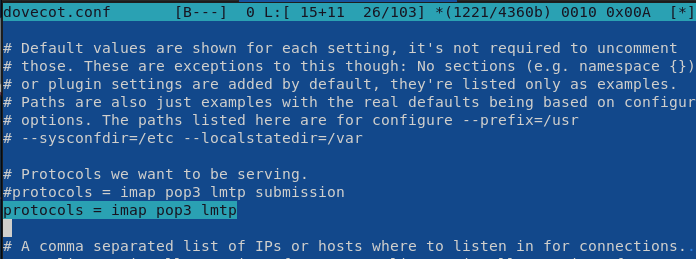
sudo -i

tail -f /var/log/maillog

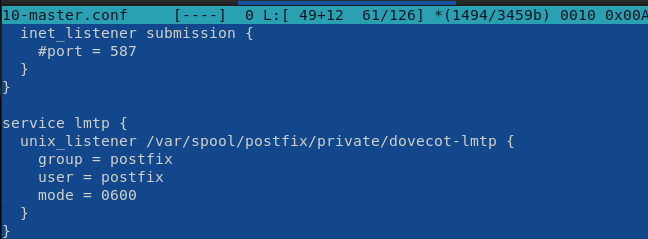


1. Добавьте в список протоколов, с которыми может работать Dovecot, протокол LMTP. Для этого в файле /etc/dovecot/dovecot.conf укажите

protocols = imap pop3 lmtp



1. Настройте 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:



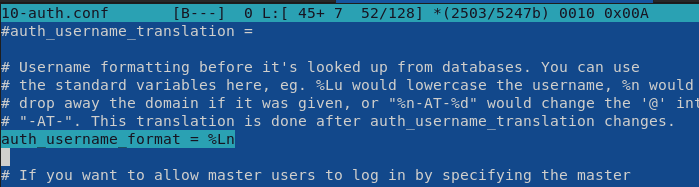
1. Переопределите в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокет:

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



1. В файле /etc/dovecot/conf.d/10-auth.conf задайте формат имени пользователя для аутентификации в форме логина пользователя без указания домена:

auth\_username\_format = %Ln



1. Перезапустите Postfix и Dovecot:

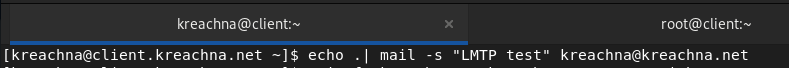
systemctl restart postfix

systemctl restart dovecot



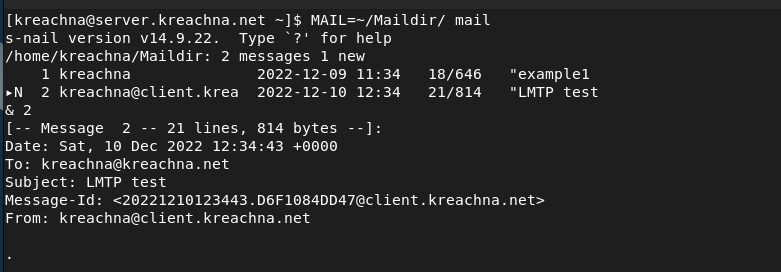
1. Из-под учётной записи своего пользователя отправьте письмо с клиента:

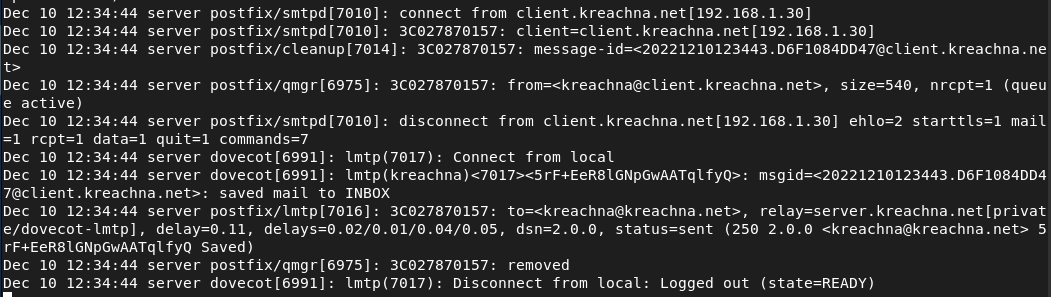
Echo .| mail -s "LMTP test" [kreachna@kreachna.net](mailto:kreachna@kreachna.net)



1. На сервере просмотрите почтовый ящик пользователя:

MAIL=~/Maildir/ mail





1. **Настройка SMTP-аутентификации**
2. В файле /etc/dovecot/conf.d/10-master.conf определите службу аутентификации пользователей:

****

1. Для Postfix задайте тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету:



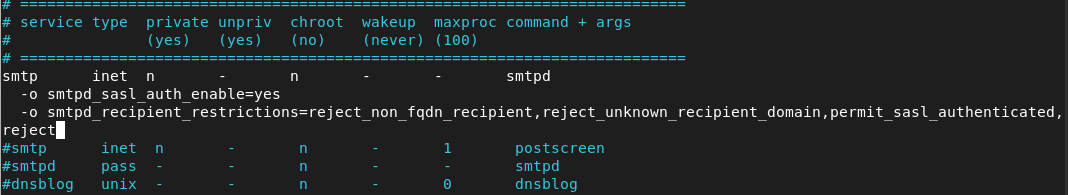
1. Настройте Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины (имеется в виду локальных пользователей сервера), обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок (порядок указания опций имеет значение):



1. В настройках Postfix ограничьте приём почты только локальным адресом SMTP-сервера сети:



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

****

1. Перезапустите Postfix и Dovecot:

systemctl restart postfix

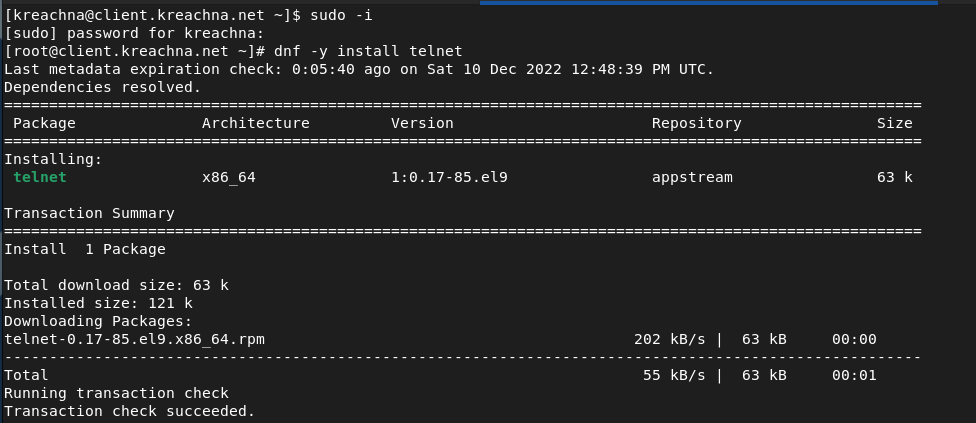
systemctl restart dovecot



1. На клиенте установите telnet:

sudo -i

dnf -y install telnet



1. На клиенте получите строку для аутентификации, вместо username указав логин вашего пользователя, а вместо password указав пароль этого пользователя:

printf 'kreachna\x00kreachna\x00123456' | base64



1. Подключитесь на клиенте к SMTP-серверу посредством telnet (вместо user укажите ваш логин):

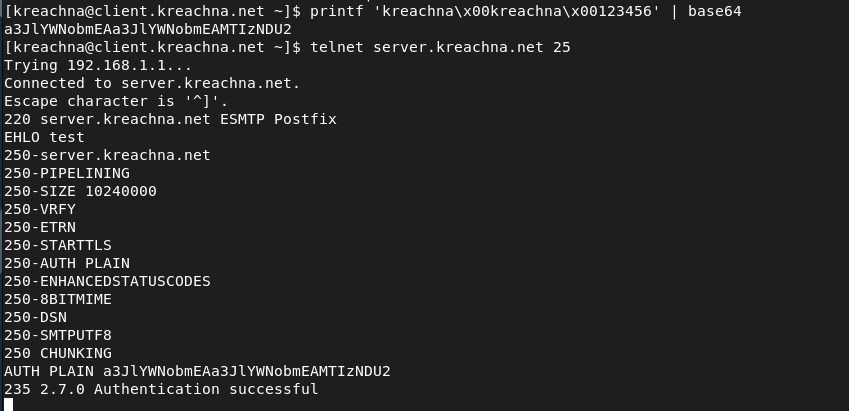
telnet server.user.net 25

Протестируйте соединение, введя

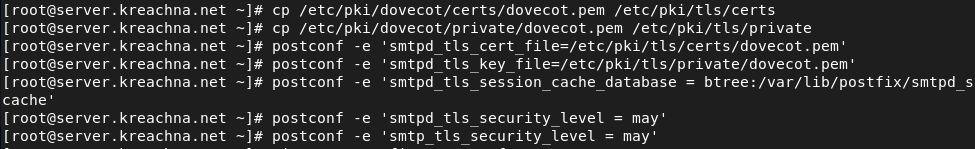
EHLO test

Проверьте авторизацию, задав:

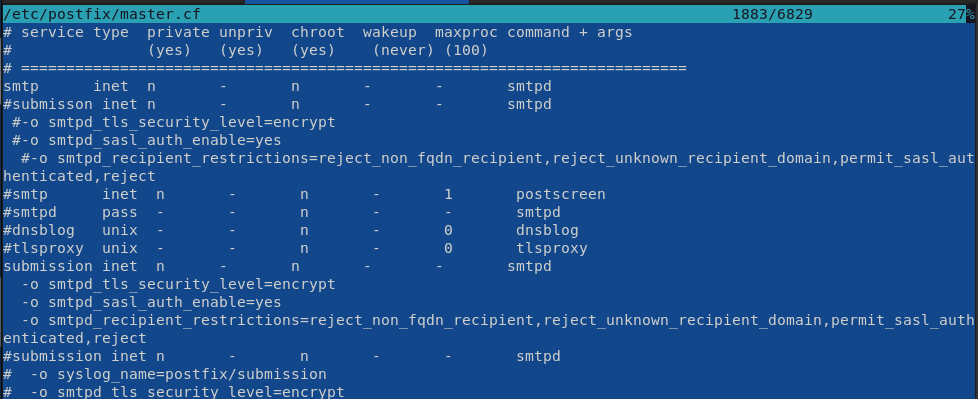
AUTH PLAIN



1. **Настройка SMTP over TLS**
2. Настройте на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно скопируйте необходимые файлы сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги (чтобы не было проблем с SELinux):



1. Для того чтобы запустить SMTP-сервер на 587-м порту, в файле /etc/postfix/master.cf замените строки



1. Настройте межсетевой экран, разрешив работать службе smtp-submission:

firewall-cmd --get-services

firewall-cmd --add-service=smtp-submission

firewall-cmd --add-service=smtp-submission --permanent

firewall-cmd –reload



1. Перезапустите Postfix:

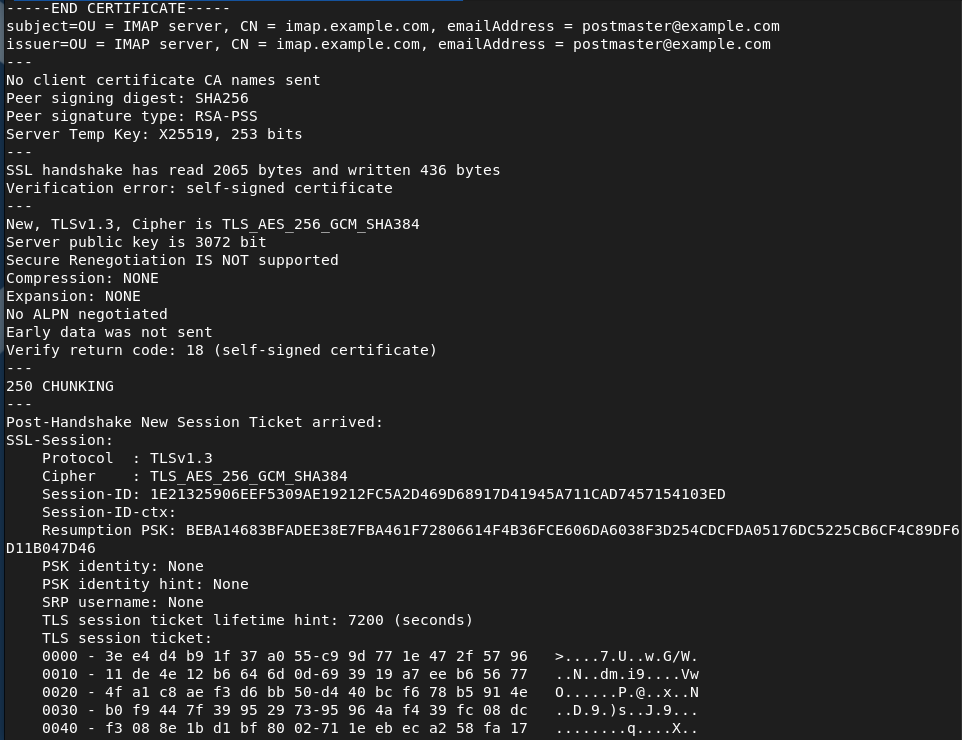
systemctl restart postfix



1. На клиенте подключитесь к SMTP-серверу через 587-й порт посредством openssl (вместо user используйте свой логин):

openssl s\_client -starttls smtp -crlf -connect server.kreachna.net:587



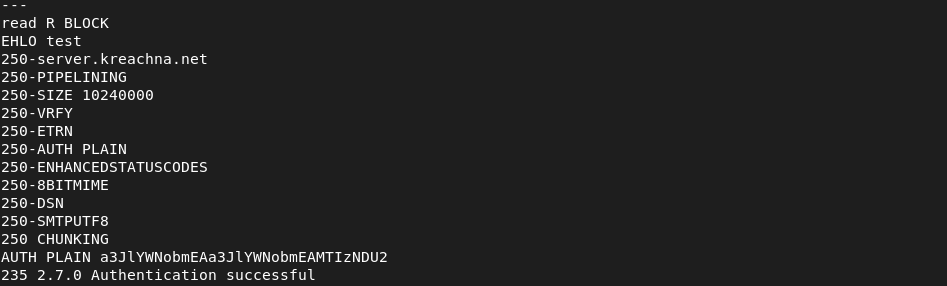


Протестируйте подключение по telnet:

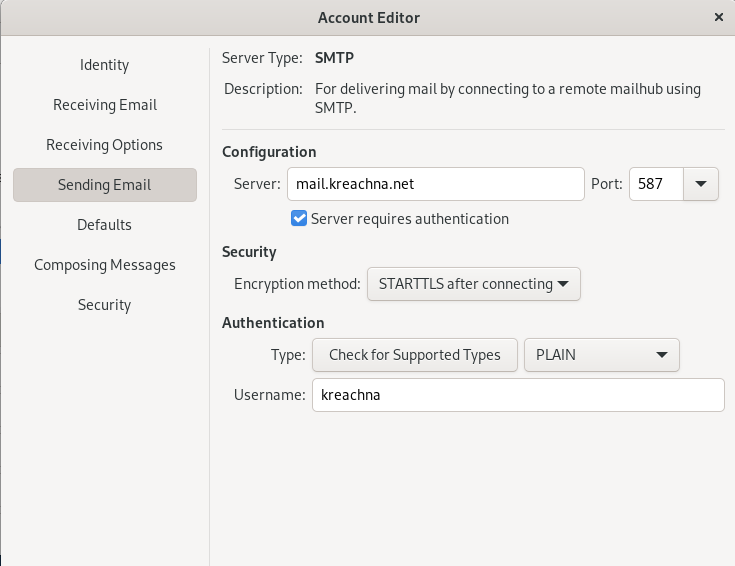
EHLO test

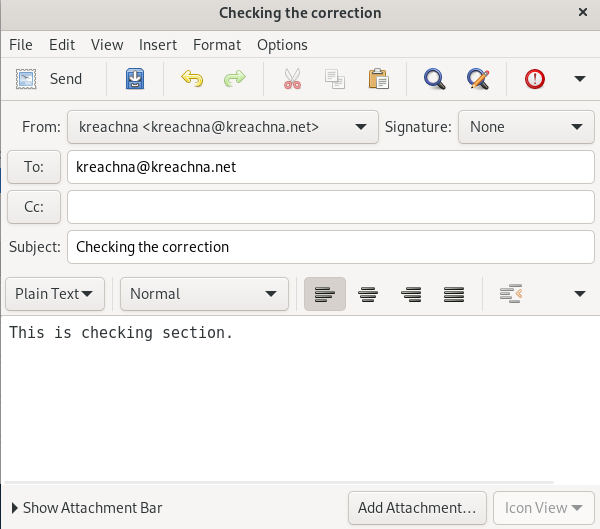
Проверьте аутентификацию:

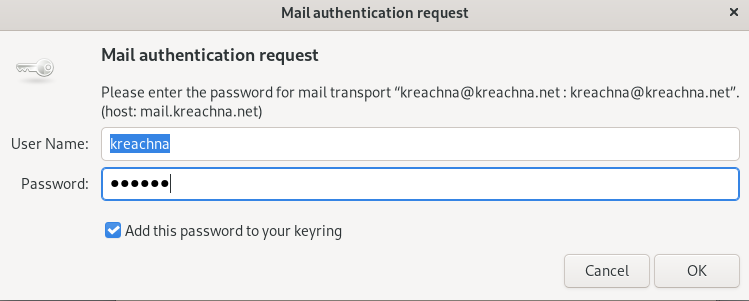
AUTH PLAIN <строка для аутентификации>

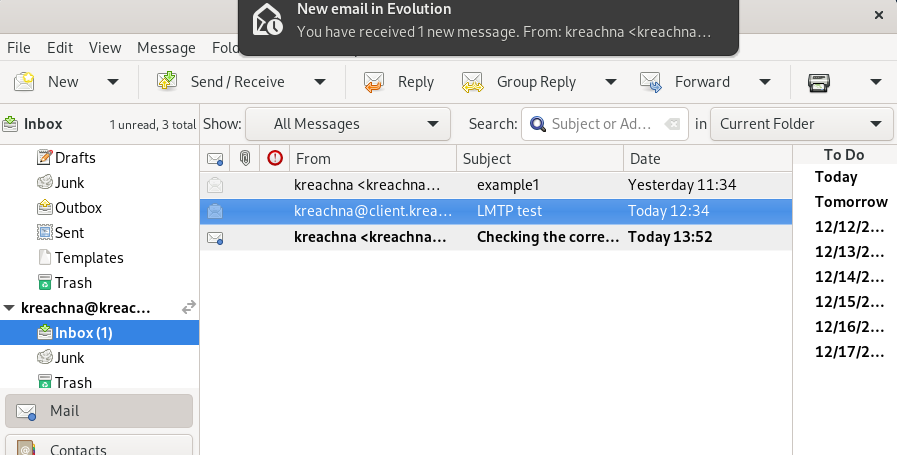


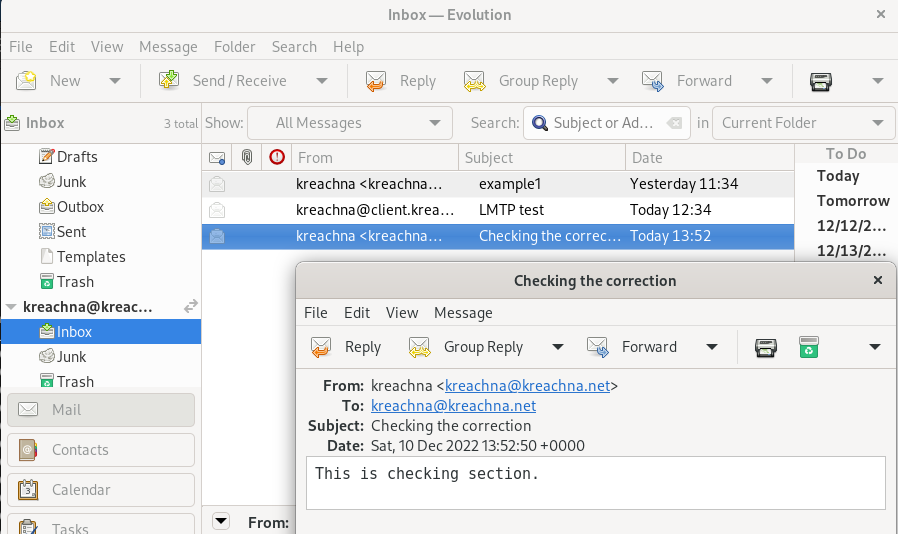
1. Проверьте корректность отправки почтовых сообщений с клиента посредством почтового клиента Evolution, предварительно скорректировав настройки учётной записи, а именно для SMTP-сервера укажите порт 587, STARTTLS и обычный пароль.

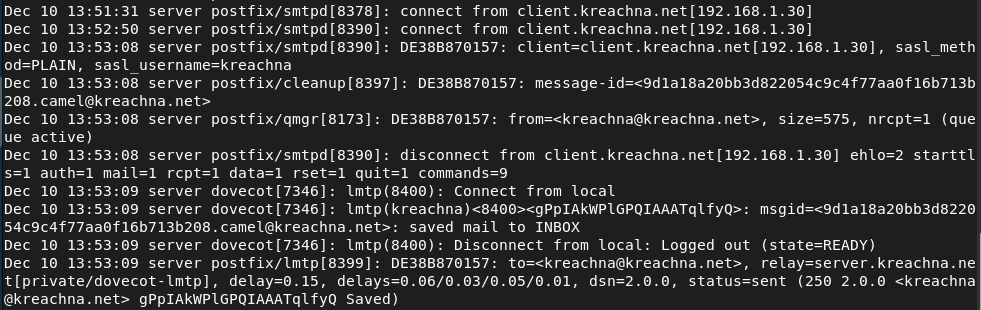
****

****

****

****

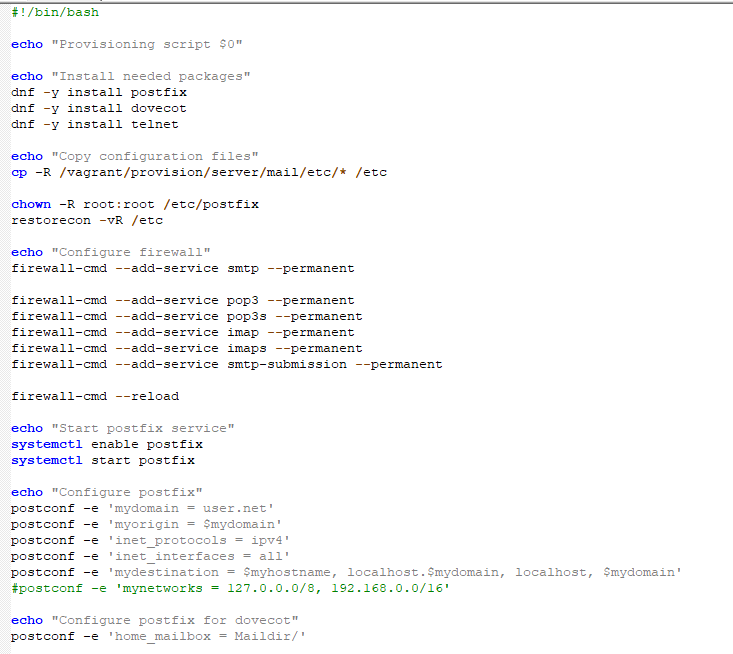
****

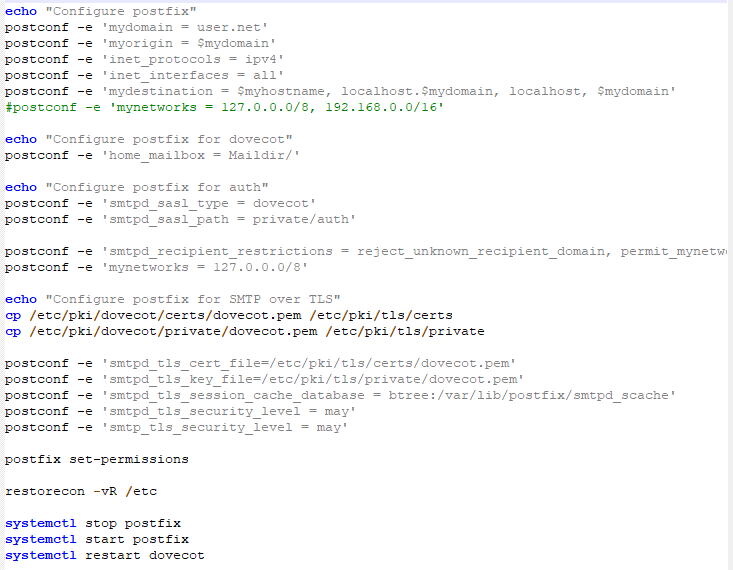


1. **Внесение изменений в настройки внутреннего окружения виртуальной машины**
2. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/. В соответствующие подкаталоги поместите конфигурационные файлы Dovecot и Postfix:

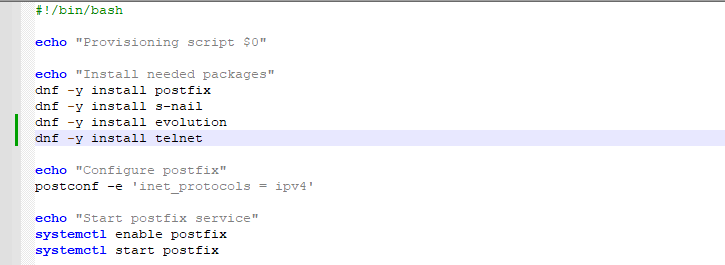


1. Внесите соответствующие изменения по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh:





1. Внесите изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet.

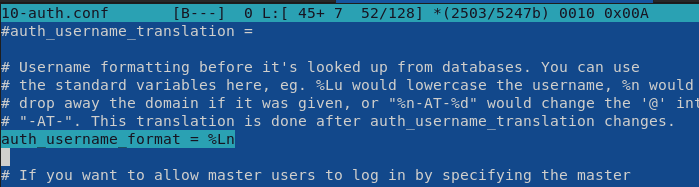


**Ответ на контрольные вопросы:**

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

Auth\_username\_format = %Ln

В файле /etc/dovecot/conf.d/10-auth.conf в ходе лабораторной работы мы задавали формат имени пользователя для аутентификации в форме логина без указания домена. За это отвечает добавление «n». Для того, чтобы задать формат в форме логина с указанием домена, нужно не указывать данную опцию.

****

1. Какие функции выполняет почтовый Relay-сервер?

Это сервер-посредник, принимающий электронную почту у отправителей и доставляющий ее получателям. Обеспечивает приём сообщения, временное хранение пересылку сообщения узлу-получателю.

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

Чрезмерное расходование трафика третьими лицами, массовые вредоносные рассылки, организации атак на отказ в обслуживании на другие почтовые системы, неиспользуемые службы и открытые порты, утечки информации.

**Вывод:**

Приобрела практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.