Отчёт по лабораторной работе 10

Расширенные настройкиSMTP-сервера

Суннатилло Махмудов

Содержание

# 1 Цель работы

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

# 2 Теоретические сведения

Почтовая система в Linux строится на взаимодействии нескольких компонентов, каждый из которых выполняет определённую функцию в процессе передачи, хранения и получения электронных сообщений.  
Основу системы составляют два ключевых сервера — **Postfix** и **Dovecot**.

**Postfix** — это почтовый транспортный агент (MTA, Mail Transfer Agent), который отвечает за приём, маршрутизацию и доставку электронной почты.  
Он реализует протокол **SMTP (Simple Mail Transfer Protocol)**, обеспечивающий передачу сообщений между серверами.  
Postfix также может выполнять функции **Relay-сервера**, пересылая почту между доменами, и поддерживает аутентификацию пользователей через **SASL (Simple Authentication and Security Layer)**.

**Dovecot** — это сервер почтовых ящиков (MDA, Mail Delivery Agent) и IMAP/POP3-сервер, обеспечивающий доступ пользователей к их сообщениям.  
Он принимает почту от Postfix через протокол **LMTP (Local Mail Transfer Protocol)** и сохраняет её в каталоге почтового ящика пользователя, чаще всего в формате **Maildir**.  
Dovecot также реализует механизмы аутентификации пользователей и шифрования с помощью **TLS (Transport Layer Security)**.

Для обеспечения безопасного обмена почтой между клиентом и сервером применяется протокол **SMTP over TLS**, который шифрует данные на уровне транспортного соединения, предотвращая перехват логинов, паролей и содержимого сообщений.  
TLS использует сертификаты, позволяющие серверу подтвердить подлинность своей личности.

В процессе работы почтовой системы различают следующие основные порты и протоколы: - **25/tcp** — SMTP, используется для пересылки писем между серверами; - **143/tcp** — IMAP, обеспечивает работу с почтовыми сообщениями на сервере; - **110/tcp** — POP3, позволяет загружать письма на клиентское устройство; - **587/tcp** — Submission, используется клиентами для отправки почты с обязательным шифрованием (STARTTLS); - **993/tcp** и **995/tcp** — защищённые версии IMAPS и POP3S соответственно.

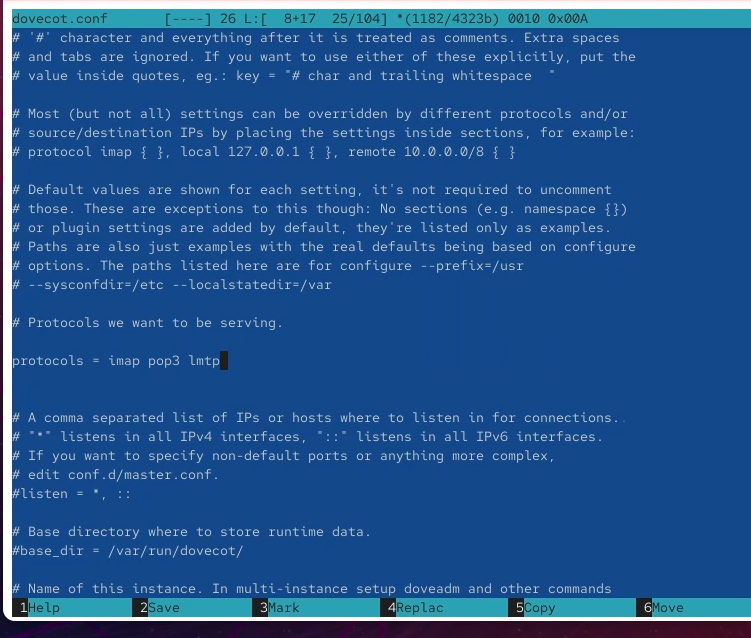
# 3 Выполнение лабораторной работы

## 3.1 Настройка LMTP в Dovecot

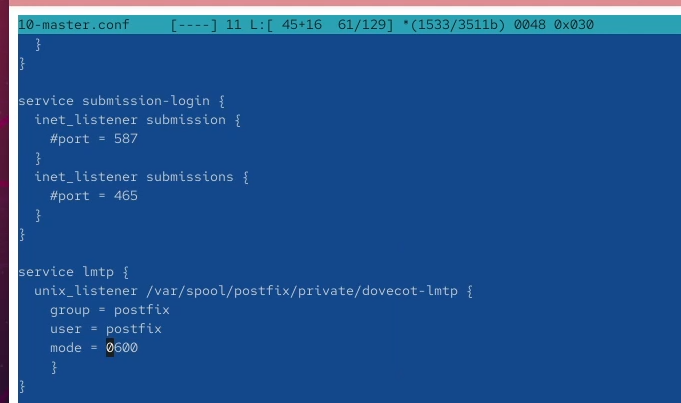
1. На виртуальной машине **server** был выполнен вход под пользователем и переход в режим суперпользователя:  
   sudo -i

* В отдельном терминале запущен мониторинг почтовой службы:  
  tail -f /var/log/maillog

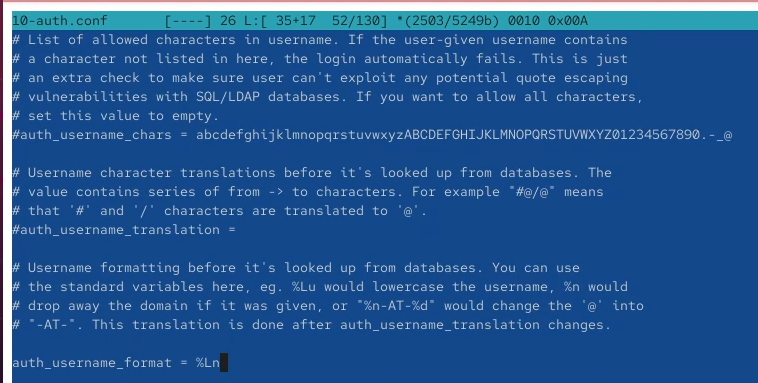
1. В конфигурационном файле **/etc/dovecot/dovecot.conf** был добавлен протокол **lmtp** в список поддерживаемых Dovecot протоколов.  
   После изменения параметр приобрёл вид:

* protocols = imap pop3 lmtp
* 
* Рис. 1: Добавление протокола LMTP в конфигурацию Dovecot

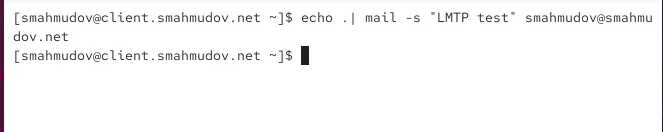
1. В файле **/etc/dovecot/conf.d/10-master.conf** был настроен сервис **lmtp** для взаимодействия с Postfix.  
   Добавлена следующая конфигурация:

* service lmtp {  
  unix\_listener /var/spool/postfix/private/dovecot-lmtp {  
  group = postfix  
  user = postfix  
  mode = 0600  
  }  
  }
* Эта настройка определяет Unix-сокет, через который Postfix передаёт сообщения Dovecot, а также права доступа и владельца.
* 
* Рис. 2: Настройка сервиса LMTP и Unix-сокета

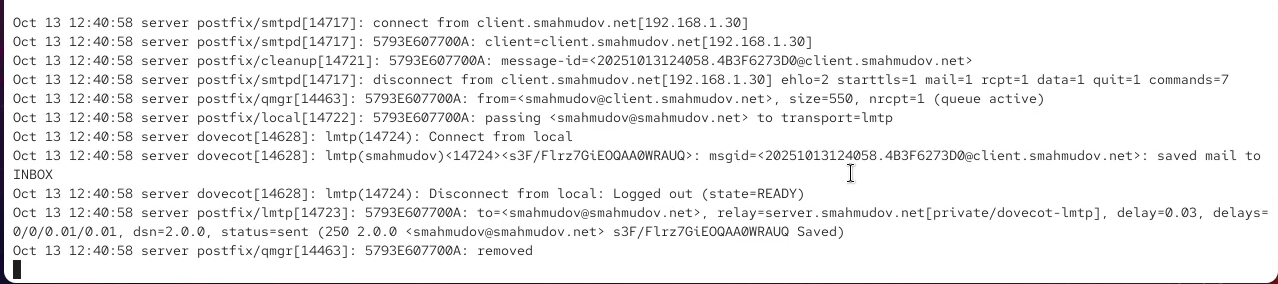
1. В файле **/etc/dovecot/conf.d/10-auth.conf** изменён формат имени пользователя для аутентификации.  
   Теперь он задаётся без доменной части:

* auth\_username\_format = %Ln
* 
* Рис. 3: Изменение формата имени пользователя для аутентификации

1. Для перенаправления локальной доставки через LMTP был выполнен постконфиг:  
   postconf -e ‘mailbox\_transport = lmtp:unix:private/dovecot-lmtp’
2. После внесённых изменений службы **Postfix** и **Dovecot** были перезапущены:  
   systemctl restart postfix  
   systemctl restart dovecot
3. С клиента, находящегося в домене **smahmudov.net**, отправлено тестовое письмо:  
   echo . | mail -s “LMTP test” smahmudov@smahmudov.net

* 
* Рис. 4: Отправка тестового письма через LMTP

1. В журнале почтового сервера наблюдалась корректная передача сообщения от клиента через Postfix к Dovecot по LMTP.  
   Из лога видно, что сообщение было успешно сохранено в почтовый ящик получателя:

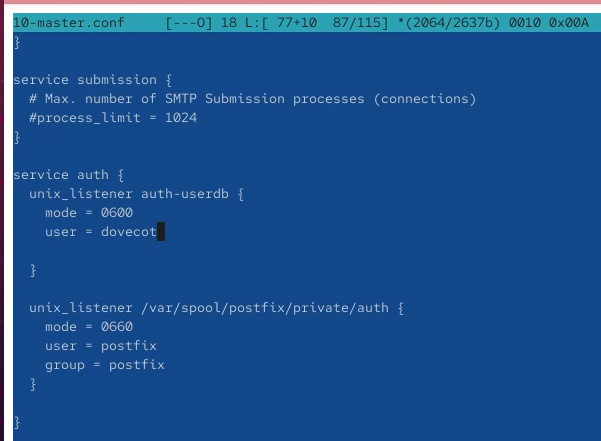
* status=sent (250 2.0.0 [smahmudov@smahmudov.net](mailto:smahmudov@smahmudov.net) s3F/FLrz7GiE0QAA0WRAUQ Saved)
* 
* Рис. 5: Фрагмент лога успешной доставки сообщения через LMTP

1. Проверка почтового ящика на сервере подтвердила получение тестового письма:  
   MAIL=~/Maildir/ mail

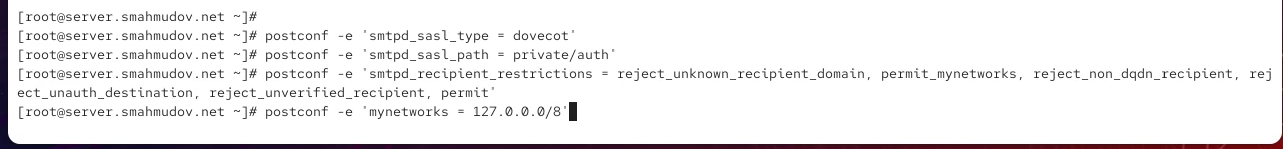
* В списке сообщений присутствует письмо с темой **“LMTP test”**, доставленное от клиента.
* 
* Рис. 6: Проверка доставки письма на сервере

## 3.2 Настройка SMTP-аутентификации

1. В файле **/etc/dovecot/conf.d/10-master.conf** была определена служба аутентификации пользователей.  
   Конфигурация включает два unix-сокета:

* service auth {  
  unix\_listener auth-userdb {  
  mode = 0600  
  user = dovecot  
  }  
  unix\_listener /var/spool/postfix/private/auth {  
  mode = 0660  
  user = postfix  
  group = postfix  
  }  
  }
* Пояснение к настройке:
  + **service auth** — определяет службу аутентификации в Dovecot.
  + **unix\_listener auth-userdb** — внутренний сокет Dovecot для обращения собственных сервисов.
  + **mode = 0600** — разрешения доступа только владельцу.
  + **user = dovecot** — владелец сокета — системный пользователь Dovecot.
  + **unix\_listener /var/spool/postfix/private/auth** — сокет для взаимодействия с Postfix.
  + **mode = 0660** — разрешения на доступ пользователю и группе.
  + **user = postfix**, **group = postfix** — предоставляют Postfix право использовать этот сокет.
* 
* Рис. 7: Определение службы аутентификации в Dovecot

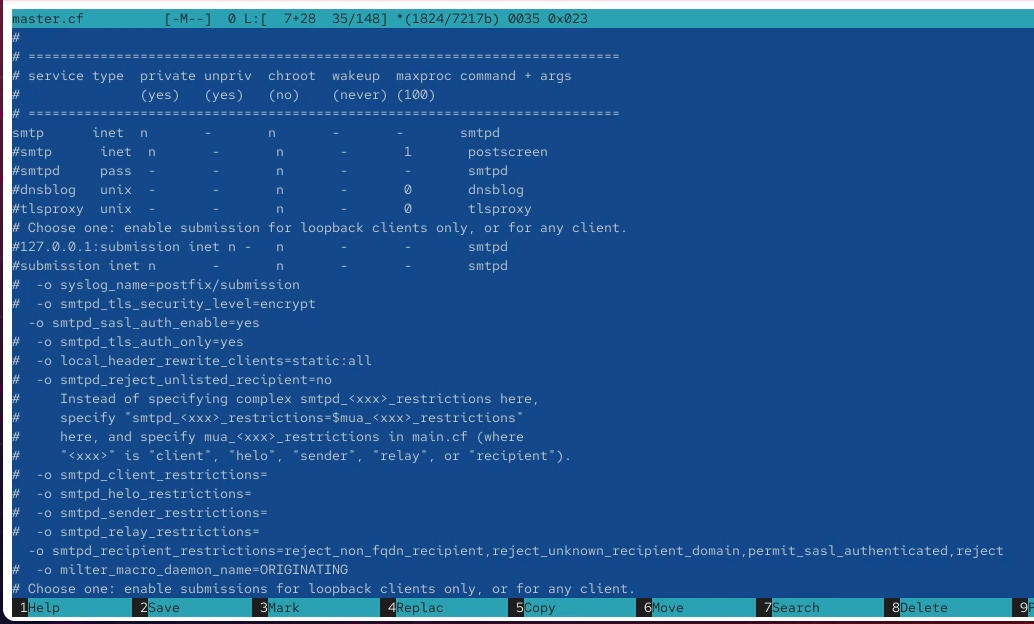
1. Для Postfix был задан тип аутентификации SASL и путь к соответствующему unix-сокету:  
   postconf -e ‘smtpd\_sasl\_type = dovecot’  
   postconf -e ‘smtpd\_sasl\_path = private/auth’

* 
* Рис. 8: Настройка SASL-аутентификации в Postfix

1. Для ограничения приёма почты и предотвращения использования сервера в качестве релея были заданы ограничения получателей:  
   postconf -e ‘smtpd\_recipient\_restrictions = reject\_unknown\_recipient\_domain, permit\_mynetworks, reject\_non\_fqdn\_recipient, reject\_unauth\_destination, reject\_unverified\_recipient, permit’

* Комментарии к опциям:
  + **reject\_unknown\_recipient\_domain** — отклоняет письма с неизвестными доменами получателей.
  + **permit\_mynetworks** — разрешает приём сообщений от доверенных сетей, определённых в mynetworks.
  + **reject\_non\_fqdn\_recipient** — запрещает использование неполных (неполных FQDN) адресов.
  + **reject\_unauth\_destination** — предотвращает пересылку писем для внешних доменов (анти-релей).
  + **reject\_unverified\_recipient** — проверяет существование получателя перед приёмом письма.
  + **permit** — разрешает приём после прохождения всех проверок.

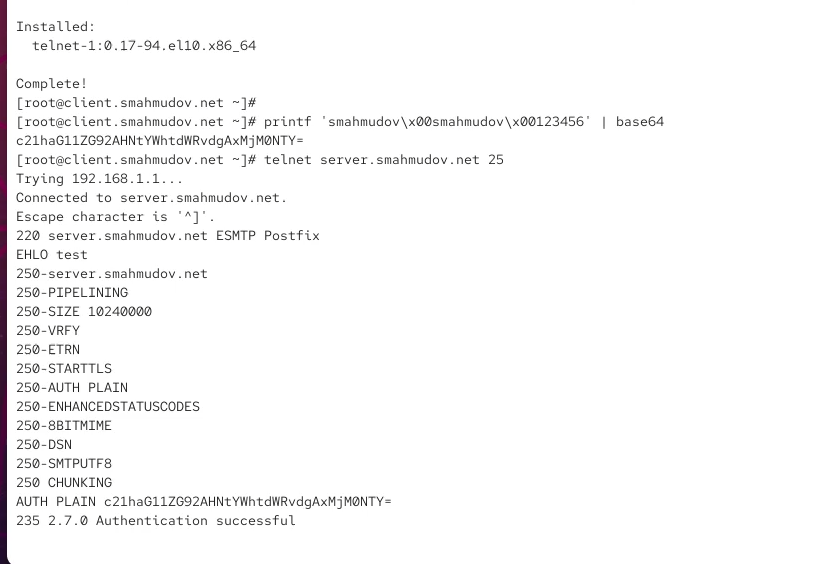
1. Для ограничения диапазона доверенной сети Postfix было выполнено:  
   postconf -e ‘mynetworks = 127.0.0.0/8’
2. Для тестирования аутентификации в файле **/etc/postfix/master.cf** была включена возможность авторизации через SASL.  
   Активирована строка для smtp-сервиса:

* smtp inet n - n - - smtpd  
  -o smtpd\_sasl\_auth\_enable=yes  
  -o smtpd\_recipient\_restrictions=reject\_non\_fqdn\_recipient,reject\_unknown\_recipient\_domain,permit\_sasl\_authenticated,reject
* 
* Рис. 9: Включение SMTP-аутентификации в master.cf

1. После настройки службы **Postfix** и **Dovecot** были перезапущены:  
   systemctl restart postfix  
   systemctl restart dovecot
2. На клиентской машине был установлен пакет **telnet** для тестирования соединения:  
   dnf -y install telnet
3. С помощью команды printf была сгенерирована строка для аутентификации пользователя **smahmudov** с паролем **123456** в кодировке base64:  
   printf 'smahmudov\x00smahmudov\x00123456' | base64

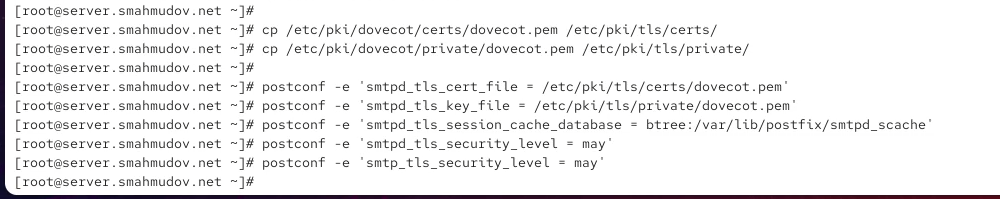
* Результат:  
  c21haG11ZG92AHNtYWhtdWRvdkAxMjM0NTY=

1. Подключение к SMTP-серверу и проверка успешной аутентификации:  
   telnet server.smahmudov.net 25  
   EHLO test  
   AUTH PLAIN c21haG11ZG92AHNtYWhtdWRvdkAxMjM0NTY=

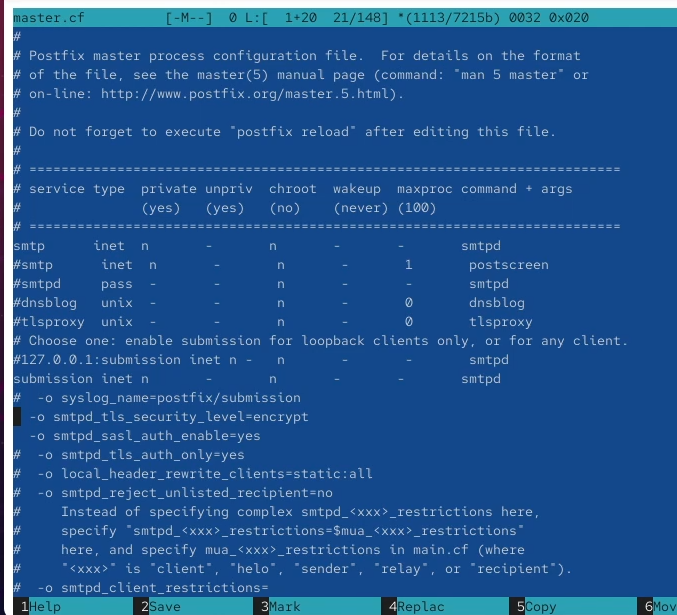
* Сервер вернул ответ:  
  **235 2.7.0 Authentication successful**, что подтверждает корректную настройку SMTP-аутентификации.
* 
* Рис. 10: Проверка SMTP-аутентификации через telnet

## 3.3 Настройка SMTP over TLS

1. На сервере был настроен TLS с использованием временного сертификата, выданного **Dovecot**.  
   Для предотвращения ошибок SELinux файлы сертификата и ключа были скопированы в стандартные каталоги TLS:

* cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs/  
  cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private/
* После этого в Postfix были указаны пути к сертификату и ключу, а также параметры кеширования TLS-сессий и уровень безопасности:
* postconf -e ‘smtpd\_tls\_cert\_file=/etc/pki/tls/certs/dovecot.pem’  
  postconf -e ‘smtpd\_tls\_key\_file=/etc/pki/tls/private/dovecot.pem’  
  postconf -e ‘smtpd\_tls\_session\_cache\_database=btree:/var/lib/postfix/smtpd\_scache’  
  postconf -e ‘smtpd\_tls\_security\_level=may’  
  postconf -e ‘smtp\_tls\_security\_level=may’
* 
* Рис. 11: Настройка TLS в Postfix и копирование сертификатов

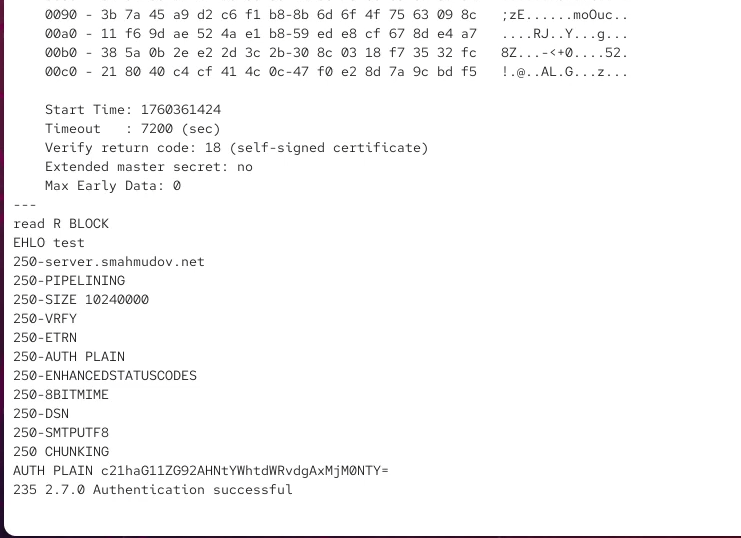
1. Для активации SMTP на порту **587** (submission) в файле **/etc/postfix/master.cf** были внесены следующие изменения.  
   Исходная запись для smtp была упрощена до:

* smtp inet n - n - - smtpd
* И добавлен новый блок для службы **submission**:
* submission inet n - n - - smtpd  
  -o smtpd\_tls\_security\_level=encrypt  
  -o smtpd\_sasl\_auth\_enable=yes  
  -o smtpd\_recipient\_restrictions=reject\_non\_fqdn\_recipient,reject\_unknown\_recipient\_domain,permit\_sasl\_authenticated,reject
* Таким образом, сервер принимает соединения на порту 587 с обязательным шифрованием и аутентификацией пользователей.
* 
* Рис. 12: Внесение изменений для SMTP submission (порт 587)

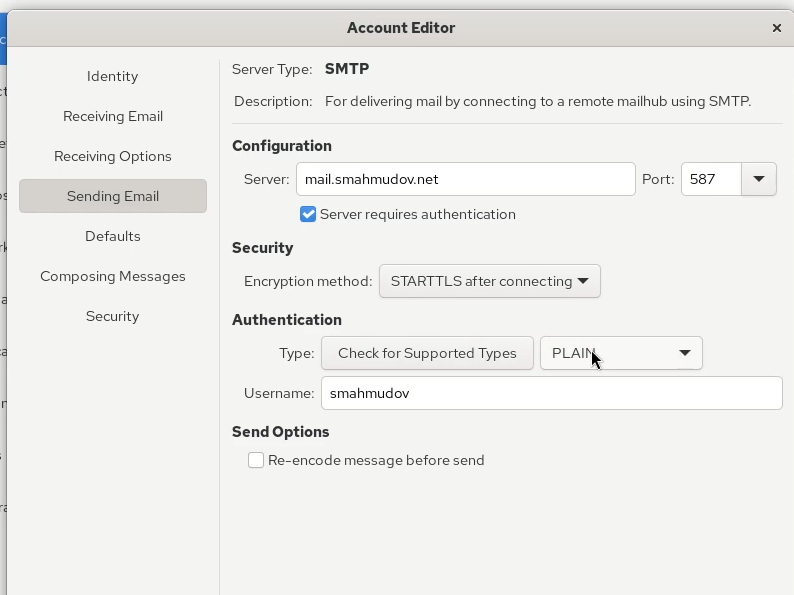
1. Для разрешения работы службы **smtp-submission** был настроен межсетевой экран:

* firewall-cmd –add-service=smtp-submission  
  firewall-cmd –add-service=smtp-submission –permanent  
  firewall-cmd –reload

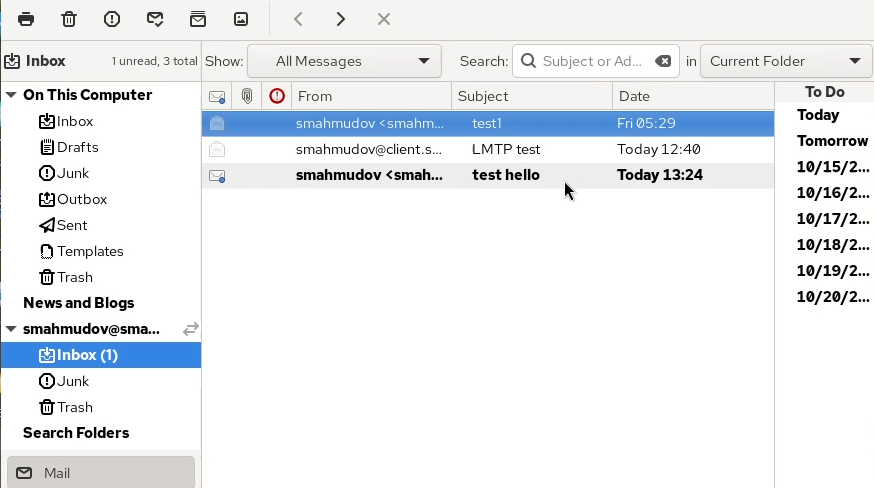
1. После внесённых изменений служба Postfix была перезапущена:  
   systemctl restart postfix
2. С клиента было выполнено тестовое подключение к SMTP-серверу через порт **587** с использованием шифрования STARTTLS:

* openssl s\_client -starttls smtp -crlf -connect server.smahmudov.net:587
* После установления защищённого соединения были выполнены команды:  
  EHLO test  
  AUTH PLAIN c21haG11ZG92AHNtYWhtdWRvdkAxMjM0NTY=
* Сервер подтвердил успешную аутентификацию:  
  **235 2.7.0 Authentication successful**
* 
* Рис. 13: Проверка аутентификации по TLS через openssl

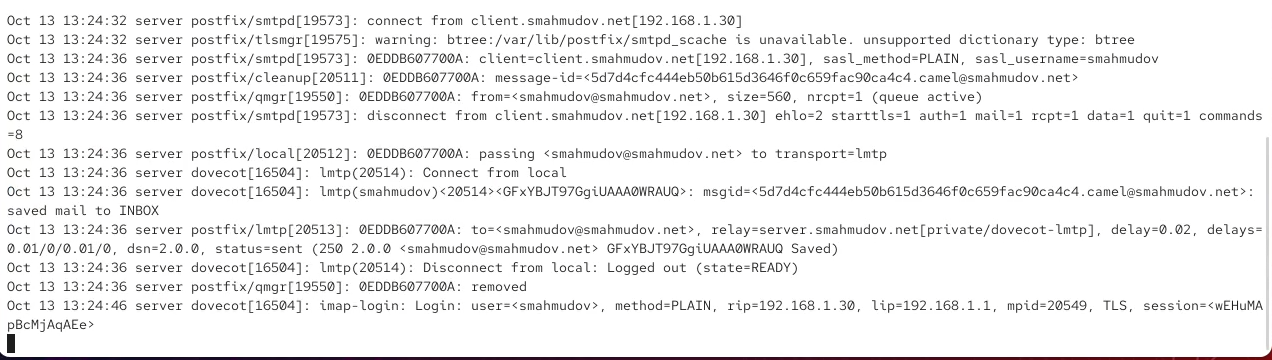
1. В почтовом клиенте **Evolution** были настроены параметры отправки почты через SMTP:
   * Сервер: *mail.smahmudov.net*
   * Порт: **587**
   * Метод шифрования: *STARTTLS after connecting*
   * Тип аутентификации: *PLAIN*
   * Имя пользователя: *smahmudov*

* 
* Рис. 14: Настройка SMTP с шифрованием в почтовом клиенте Evolution

1. После настройки был выполнен тест отправки письма.  
   Сообщение с темой **“test hello”** было успешно доставлено в почтовый ящик получателя, что подтверждает корректную работу SMTP over TLS.

* 
* Рис. 15: Успешная отправка письма через защищённый SMTP

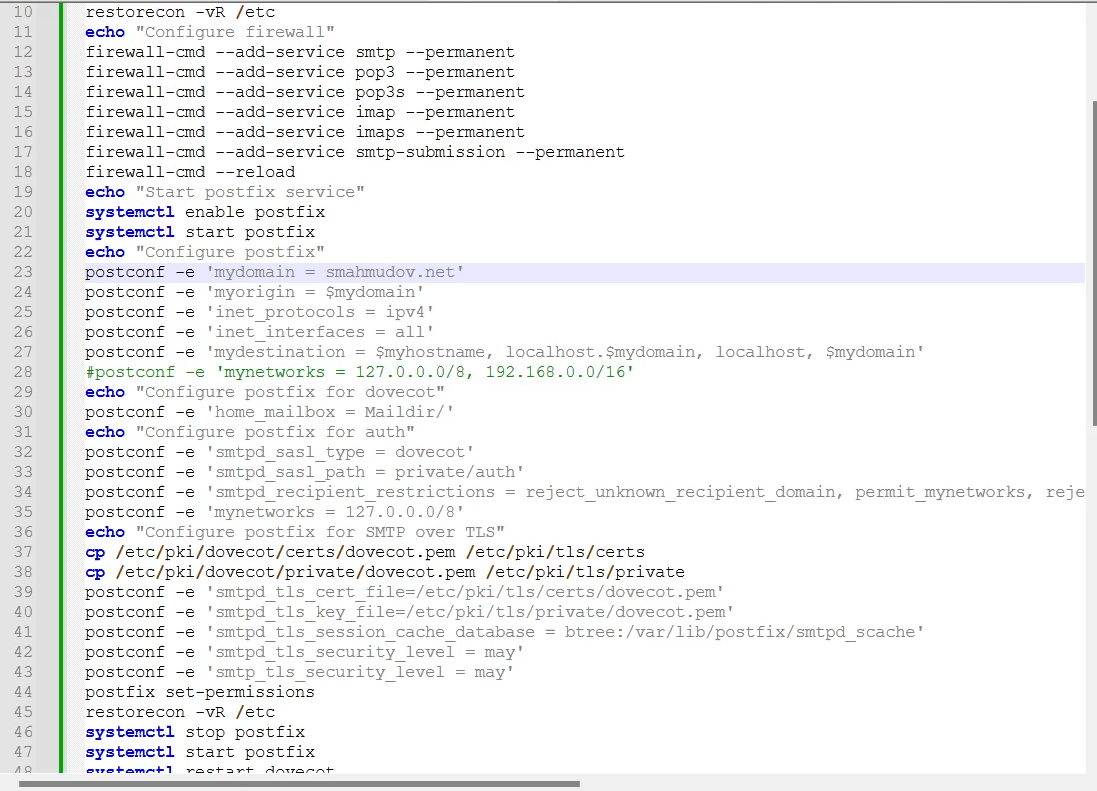
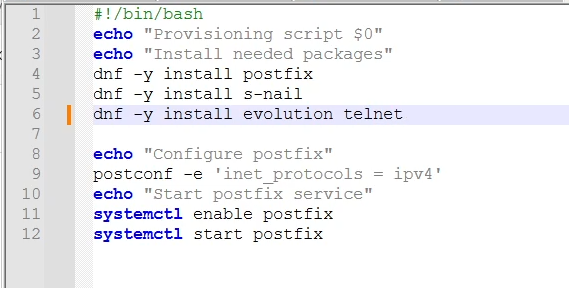
1. В логе почтового сервера видно, что соединение установлено с использованием шифрования TLS и успешной аутентификации пользователя.  
   Письмо было передано через Postfix и доставлено Dovecot в папку INBOX:

* **status=sent (250 2.0.0** [**smahmudov@smahmudov.net**](mailto:smahmudov@smahmudov.net) **Saved mail to INBOX)**
* 
* Рис. 16: Фрагмент лога успешной доставки письма через SMTP over TLS

# 4 Выполнение лабораторной работы

## 4.1 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. В подкаталог **mail/etc/dovecot/** были скопированы актуальные конфигурационные файлы Dovecot:
2. В скрипт **/vagrant/provision/server/mail.sh** были внесены изменения, обеспечивающие автоматическую установку и настройку сервисов **Postfix**, **Dovecot**, и необходимых инструментов.

* 
* Рис. 17: Скрипт для сервера
* 
* Рис. 18: Скрипт для клиента

# 5 Вывод

В ходе лабораторной работы была выполнена полная настройка почтового сервера с поддержкой **LMTP**, **SMTP-аутентификации** и **SMTP over TLS**.  
Были сконфигурированы службы **Postfix** и **Dovecot**, обеспечены защищённая передача данных и авторизация пользователей.  
Почтовый обмен успешно проверен с помощью клиента **Evolution** и инструментов **telnet** и **openssl**, подтверждая корректную работу системы.

# 6 Контрольные вопросы

1. **Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.**  
   Формат аутентификации с указанием домена задаётся в файле **/etc/dovecot/conf.d/10-auth.conf** параметром:  
   auth\_username\_format = %Lu  
   Здесь %L приводит имя пользователя к нижнему регистру, а %u означает полный логин вместе с доменом (например, *user@smahmudov.net*).
2. **Какие функции выполняет почтовый Relay-сервер?**  
   Почтовый Relay-сервер (или SMTP Relay) выполняет передачу почтовых сообщений между различными почтовыми доменами и серверами.  
   Он принимает почту от отправителя и перенаправляет её к следующему узлу сети или к серверу назначения, обеспечивая доставку сообщений за пределами локального домена.
3. **Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?**  
   Если почтовый сервер настроен как открытый Relay (Open Relay), им могут воспользоваться злоумышленники для рассылки спама или фишинговых сообщений.  
   Это приведёт к попаданию IP-адреса сервера в «чёрные списки» (RBL), снижению репутации домена и блокировке легитимных почтовых отправлений.

# 7 Список литературы

1. Postfix SASL Howto. — URL: http://www.postfix.org/SASL\_README.html (visited on 09/13/2021).