

Лабораторная работа №
Расширенные настройки SMTP-сервера
Абд эль хай мохамад

Содержание

1. Цель работы.....	2
2. Задание	2
3. Выполнение лабораторной работы.....	2
3.1 Настройка LMTP в Dovecote.....	2
3.2 Настройка SMTP-аутентификации.....	2
3.3 Настройка SMTP over TLS.....	5
4. Вывод	10
5. Контрольные вопросы.....	10

Список иллюстраций

фигура 1 protocols.....	2
фигура 3 MAIL=/Maildri/mail.....	3
фигура 4 protocols.....	4
фигура 2 telnet.....	5
фигура 5 telnet.....	6
фигура 6 openssl.....	8
фигура 7 evolution.....	9
фигура 8 evolution.....	10

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

v

3.2 Настройка SMTP-аутентификации

В файле /etc/dovecot/conf.d/10-master.conf я определил службу аутентификации пользователей:

```
service auth {  
  
  unix_listener /var/spool/postfix/private/auth {  
  
    group = postfix  
  
    user = postfix  
  
    mode = 0660  
  
  }  
  
  unix_listener auth-userdb {  
  
    mode = 0600  
  
    user = dovecot  
  
  }  
  
}
```

service auth { : Эта строка указывает на начало блока конфигурации службы аутентификации.

`unix_listener /var/spool/postfix/private/auth {`: Эта строка определяет файл сокета Unix, который будет прослушивать служба аутентификации. В данном случае путь к файлу — `/var/spool/postfix/private/auth`.

`group = postfix`: эта строка устанавливает групповое владение файлом сокета Unix группе `postfix`.

`user = postfix`: эта строка устанавливает право собственности пользователя на файл сокета Unix пользователю `postfix`.

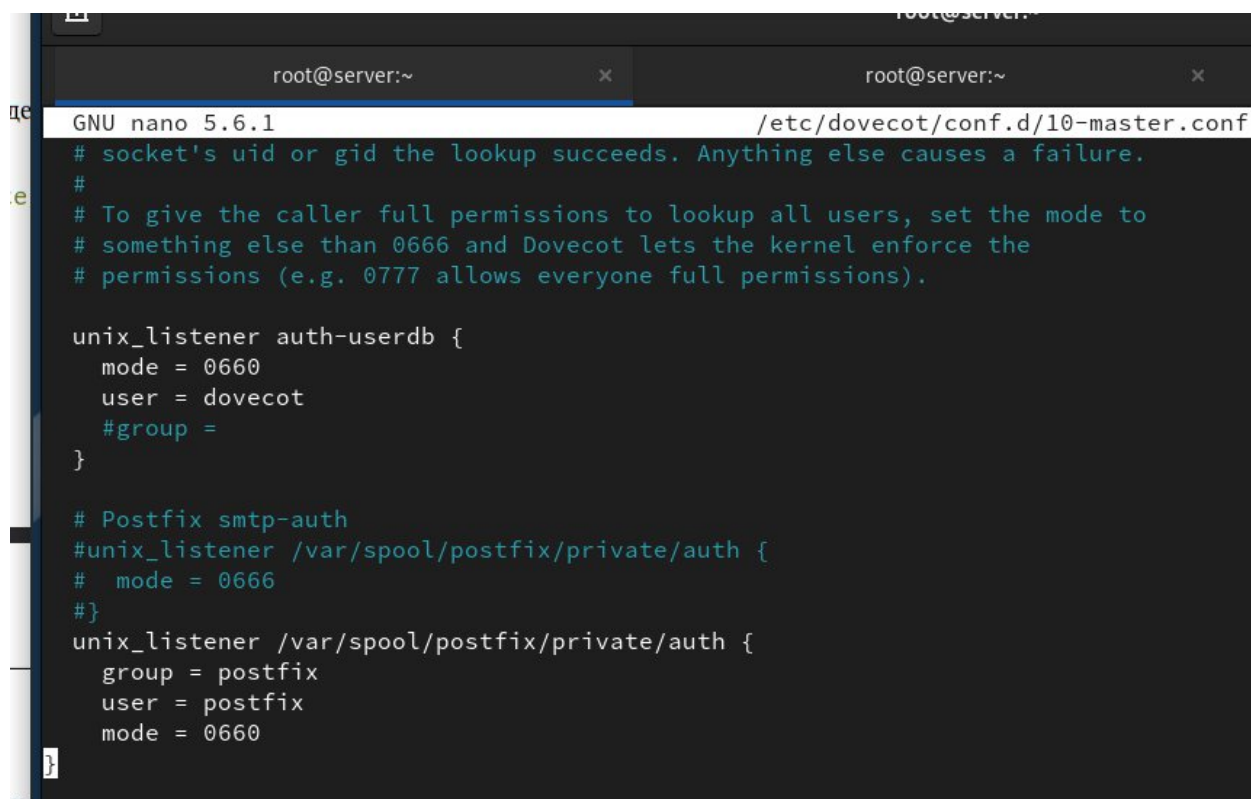
`mode = 0660`: Эта строка устанавливает разрешения файла сокета Unix на 0660, что означает, что владелец и группа имеют разрешения на чтение и запись, в то время как другие не имеют разрешений.

`unix_listener auth-userdb {`: Эта строка указывает другой файл сокета Unix, который будет прослушивать служба аутентификации. В данном случае имя файла — `auth-userdb`.

`mode = 0600`: Эта строка устанавливает права доступа к файлу сокета Unix `auth-userdb` равным 0600, что означает, что только владелец имеет разрешения на чтение и запись, в то время как другие не имеют разрешений.

`user = dovecot`: эта строка устанавливает право собственности на файл сокета Unix `auth-userdb` пользователю `dovecot`.

Приведенная выше конфигурация устанавливает два файла сокетов Unix для службы аутентификации, каждый с разными разрешениями и настройками владения.



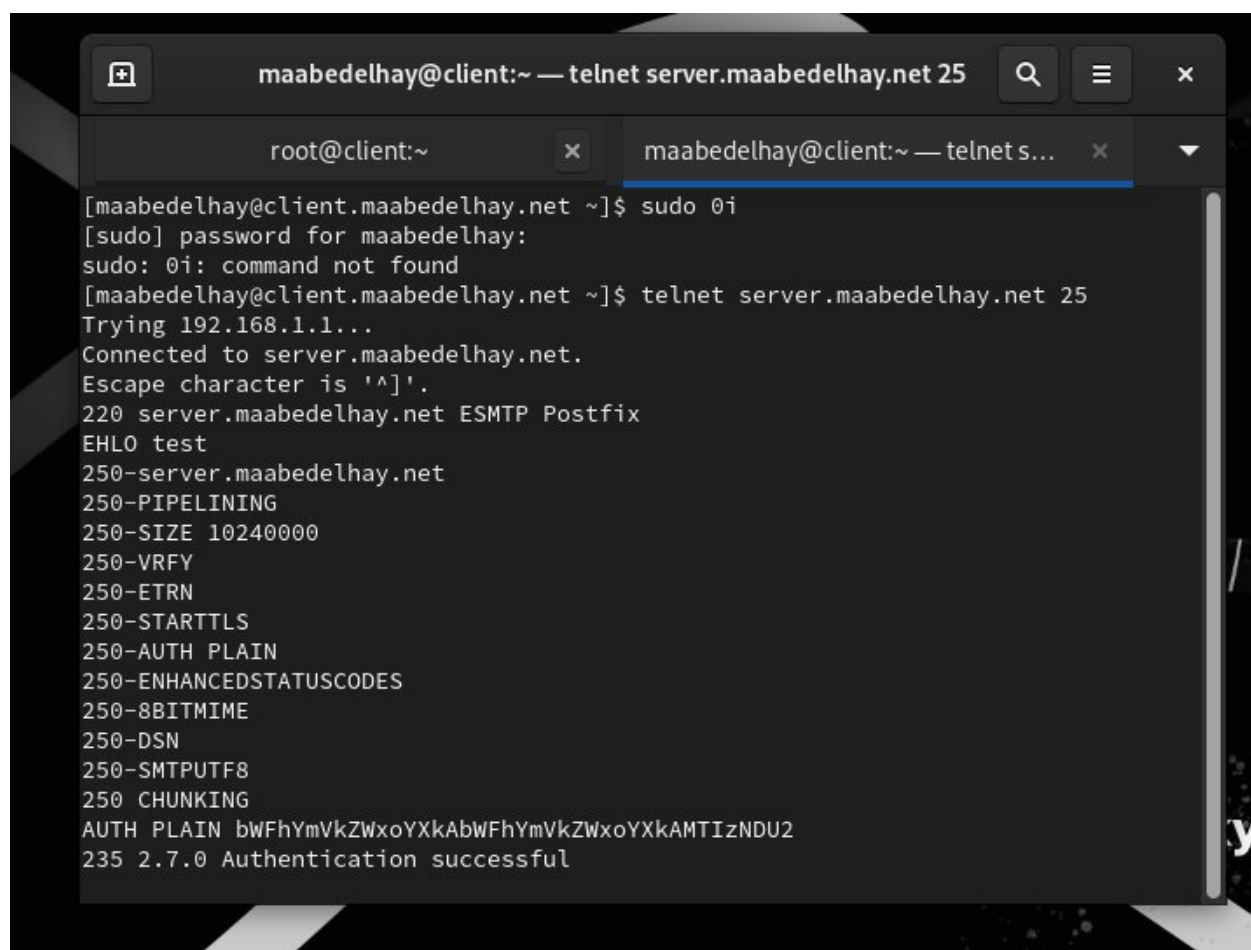
```
GNU nano 5.6.1 /etc/dovecot/conf.d/10-master.conf
# socket's uid or gid the lookup succeeds. Anything else causes a failure.
#
# To give the caller full permissions to lookup all users, set the mode to
# something else than 0666 and Dovecot lets the kernel enforce the
# permissions (e.g. 0777 allows everyone full permissions).

unix_listener auth-userdb {
    mode = 0660
    user = dovecot
    #group =
}

# Postfix smtp-auth
#unix_listener /var/spool/postfix/private/auth {
#    mode = 0666
#}
unix_listener /var/spool/postfix/private/auth {
    group = postfix
    user = postfix
    mode = 0660
}
```

фигура 4 protocols

подключился к почтовому серверу с виртуальной клиентской машины по телнету



```
maabeldelhay@client:~ — telnet server.maabeldelhay.net 25
root@client:~
[maabeldelhay@client.maabeldelhay.net ~]$ sudo 0i
[sudo] password for maabeldelhay:
sudo: 0i: command not found
[maabeldelhay@client.maabeldelhay.net ~]$ telnet server.maabeldelhay.net 25
Trying 192.168.1.1...
Connected to server.maabeldelhay.net.
Escape character is '^]'.
220 server.maabeldelhay.net ESMTP Postfix
EHLO test
250-server.maabeldelhay.net
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN bWfhYmVkZWxoYXkAbWfhYmVkZWxoYXkAMTIzNDU2
235 2.7.0 Authentication successful
```

фигура 2 telnet

Чтобы сгенерировать текст аутентификации, я использовал следующую команду

```
printf 'maabeldelhay\maabeldelhay\x00123456' | база64
```

телнет server.user.net 25

Проверьте соединение, введя

ЭХЛО-тест

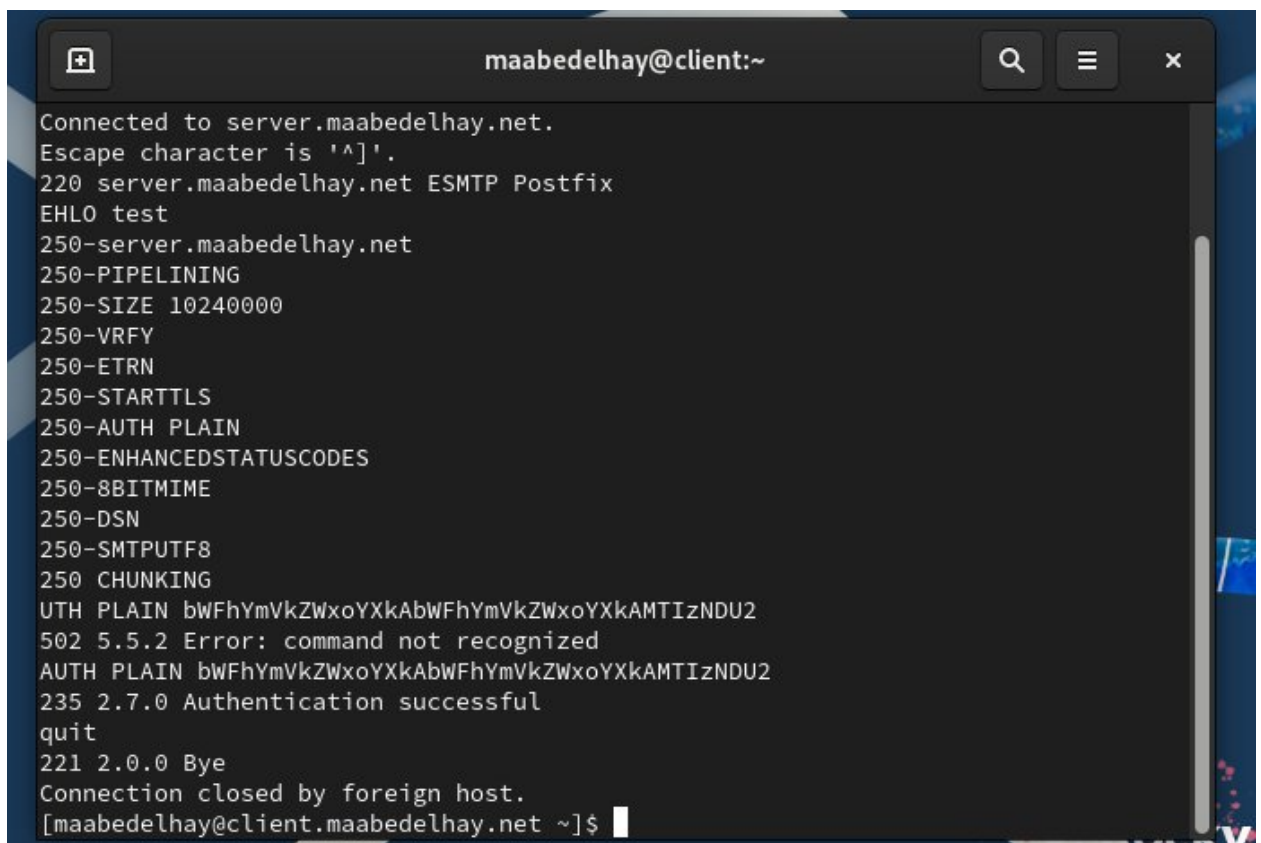
Проверьте авторизацию, установив:

AUTH PLAIN <строка для аутентификации>

Например, для пользователя пользователя:

АУТИЗАЦИЯ PLAIN dXNlcgB1c2VyADEyMzQ1Ng==

Завершить сеанс Telnet на клиенте



```
maabeldelhay@client:~
Connected to server.maabeldelhay.net.
Escape character is '^]'.
220 server.maabeldelhay.net ESMTP Postfix
EHLO test
250-server.maabeldelhay.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN bWfhYmVkdWxoYXkAbWfhYmVkdWxoYXkAMTIzNDU2
502 5.5.2 Error: command not recognized
AUTH PLAIN bWfhYmVkdWxoYXkAbWfhYmVkdWxoYXkAMTIzNDU2
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
Connection closed by foreign host.
[maabeldelhay@client.maabeldelhay.net ~]$
```

фигура 5 telnet

3.3 Настройка SMTP over TLS

Настройте на сервере TLS, воспользовавшись временным сертификатом Dovecot.

Предварительно скопируйте необходимые файлы сертификата и ключа из катало-

га /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги

(чтобы не было проблем с SELinux):

```
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
```

```
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
```

Сконфигурируйте Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения 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 =
```

```
btrees:/var/lib/postfix/smtpd_scache'↔
```

```
postconf -e 'smtpd_tls_security_level = may'
```

```
postconf -e 'smtp_tls_security_level = may'
```

2. Для того чтобы запустить SMTP-сервер на 587-м порту, в файле

/etc/postfix/master.cf заменил строки

```
smtp inet n - n - smtpd
```

```
-o smtpd_sasl_auth_enable=yes
```

```
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient,rej ]
```

```
ect_unknown_recipient_domain,permit_sasl_authenticated,reject↔
```

на следующую запись:

```
smtp inet n - n - smtpd
```

и добавил следующие строки:

```
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,rej ]
```

```
ect_unknown_recipient_domain,permit_sasl_authenticated,reject↔
```

3. Настройл межсетевой экран, разрешив работать службе smtp-submission:

```
firewall-cmd --get-services
```

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

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

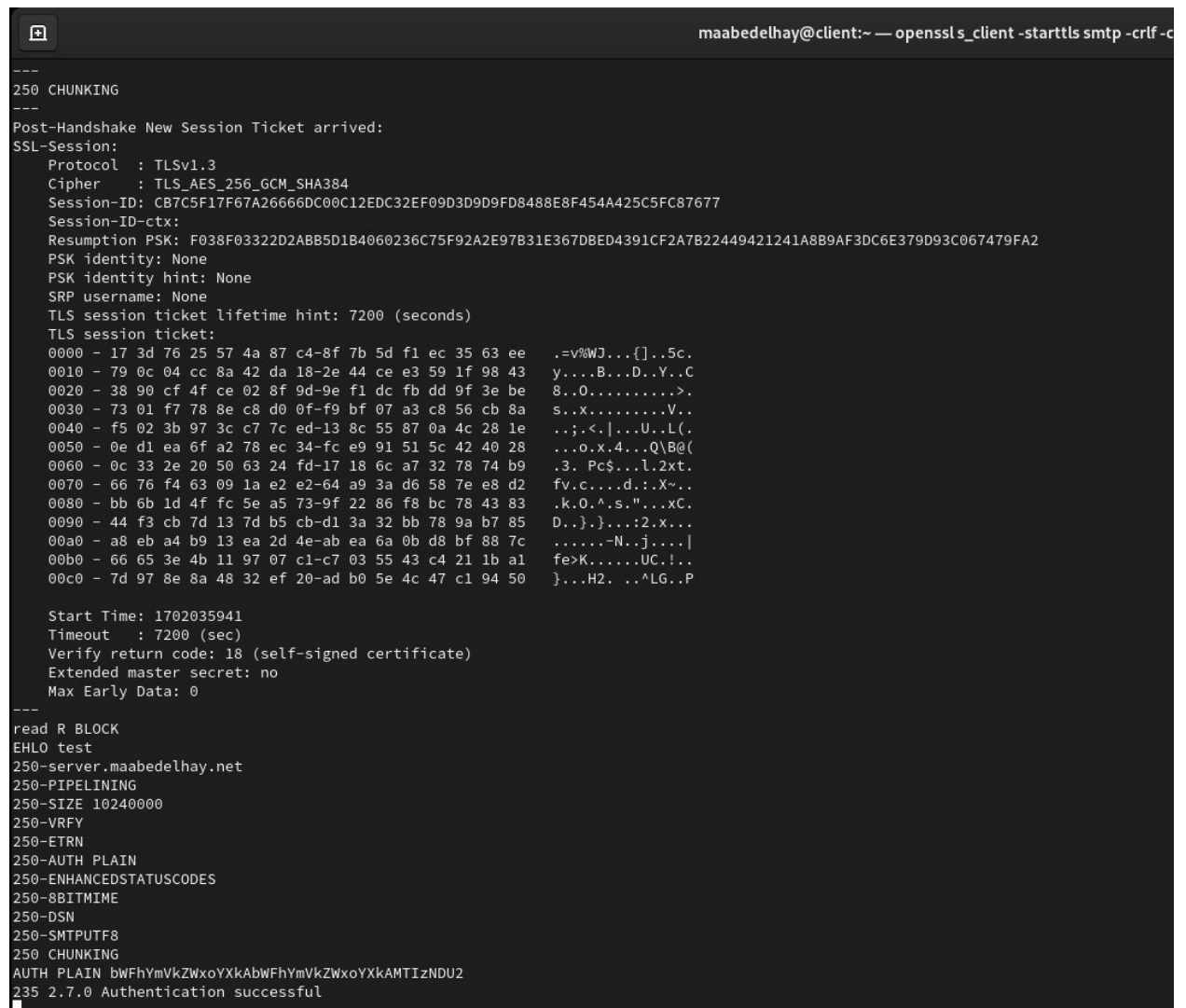
firewall-cmd --reload

4. Перезапустил Postfix:

systemctl restart postfix

5. На клиенте я подключился к SMTP-серверу через порт 587, используя openssl :

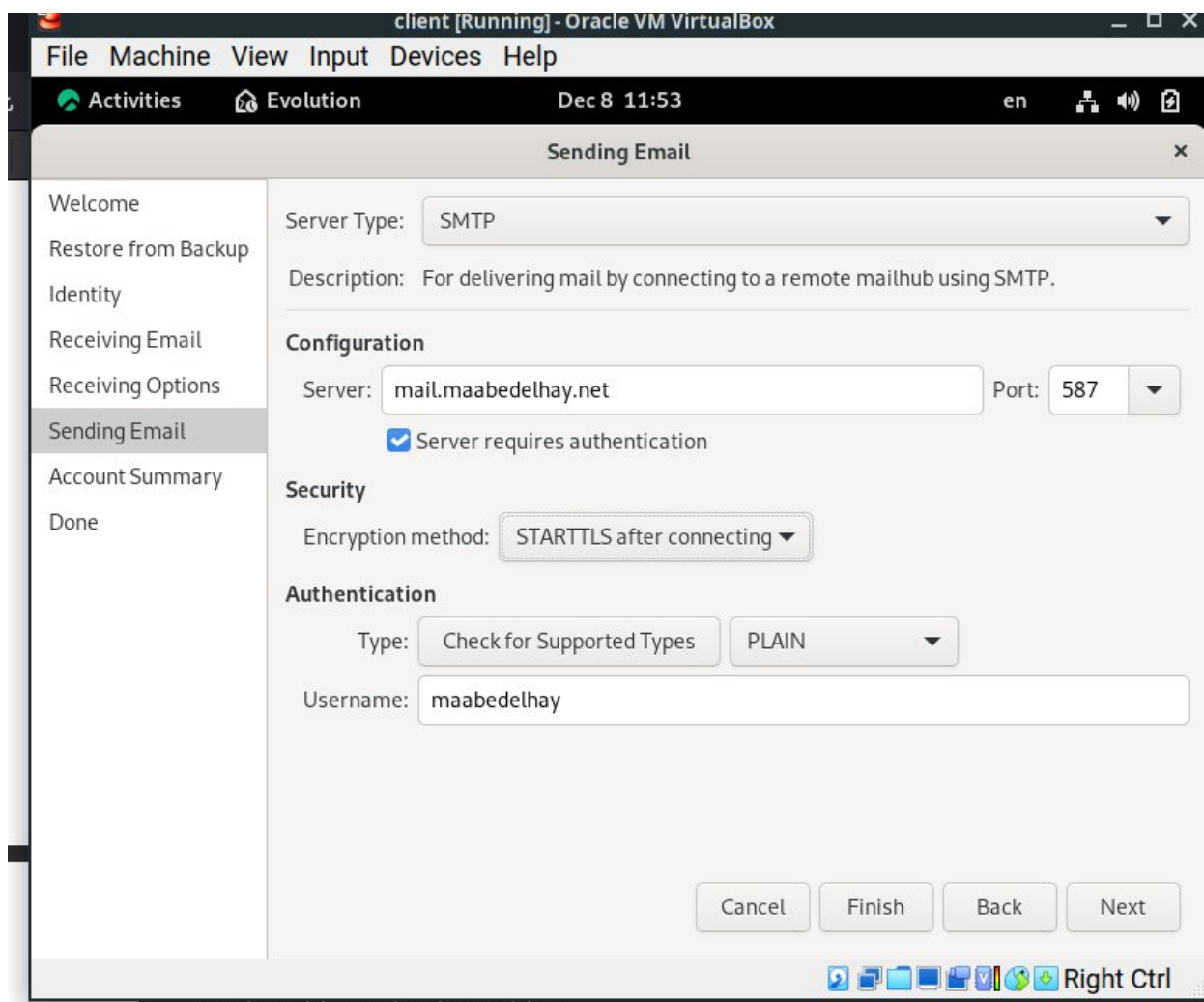
openssl s_client -starttls smtp -crlf -connect server.maabeldelhay.net:587



```
maabeldelhay@client:~ — openssl s_client -starttls smtp -crlf -c
---
250 CHUNKING
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol : TLSv1.3
    Cipher   : TLS_AES_256_GCM_SHA384
    Session-ID: CB7C5F17F67A2666DC00C12EDC32EF09D3D9D9FD8488E8F454A425C5FC87677
    Session-ID-ctx:
    Resumption PSK: F038F0332D2ABB5D1B4060236C75F92A2E97B31E367DBED4391CF2A7B22449421241A8B9AF3DC6E379D93C067479FA2
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 17 3d 76 25 57 4a 87 c4-8f 7b 5d f1 ec 35 63 ee      . = v % W J . . . { } . . 5 c .
    0010 - 79 0c 04 cc 8a 42 da 18-2e 44 ce e3 59 1f 98 43      y . . . . B . . . D . . Y . . C
    0020 - 38 90 cf 4f ce 02 8f 9d-9e f1 dc fb dd 9f 3e be      8 . . 0 . . . . . . . . . . > .
    0030 - 73 01 f7 78 8e c8 d0 0f-f9 bf 07 a3 c8 56 cb 8a      s . . x . . . . . . . . . . V . .
    0040 - f5 02 3b 97 3c c7 7c ed-13 8c 55 87 0a 4c 28 1e      . . ; . < . | . . . U . . L ( .
    0050 - 0e d1 ea 6f a2 78 ec 34-fc e9 91 51 5c 42 40 28      . . . . o . x . 4 . . . Q \ B @ (
    0060 - 0c 33 2e 20 50 63 24 fd-17 18 6c a7 32 78 74 b9      . 3 . P c $ . . . . l . 2 x t .
    0070 - 66 76 f4 63 09 1a e2 e2-64 a9 3a d6 58 7e e8 d2      f v . c . . . . d . : . X ~ . .
    0080 - bb 6b 1d 4f fc 5e a5 73-9f 22 86 f8 bc 78 43 83      . k . 0 . ^ . s . " . . . x C .
    0090 - 44 f3 cb 7d 13 7d b5 cb-d1 3a 32 bb 78 9a b7 85      D . . } . } . . . . 2 . x . .
    00a0 - a8 eb a4 b9 13 ea 2d 4e-ab ea 6a 0b d8 bf 88 7c      . . . . . - N . . j . . . . |
    00b0 - 66 65 3e 4b 11 97 07 c1-c7 03 55 43 c4 21 1b a1      f e > K . . . . . U C . ! . .
    00c0 - 7d 97 8e 8a 48 32 ef 20-ad b0 5e 4c 47 c1 94 50      } . . H 2 . . . ^ L G . . P

    Start Time: 1702035941
    Timeout    : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
EHLO test
250-server.maabeldelhay.net
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN bWFhYmVkZWx0eXkAbWFhYmVkZWx0eXkAMTIzNDU2
235 2.7.0 Authentication successful
```

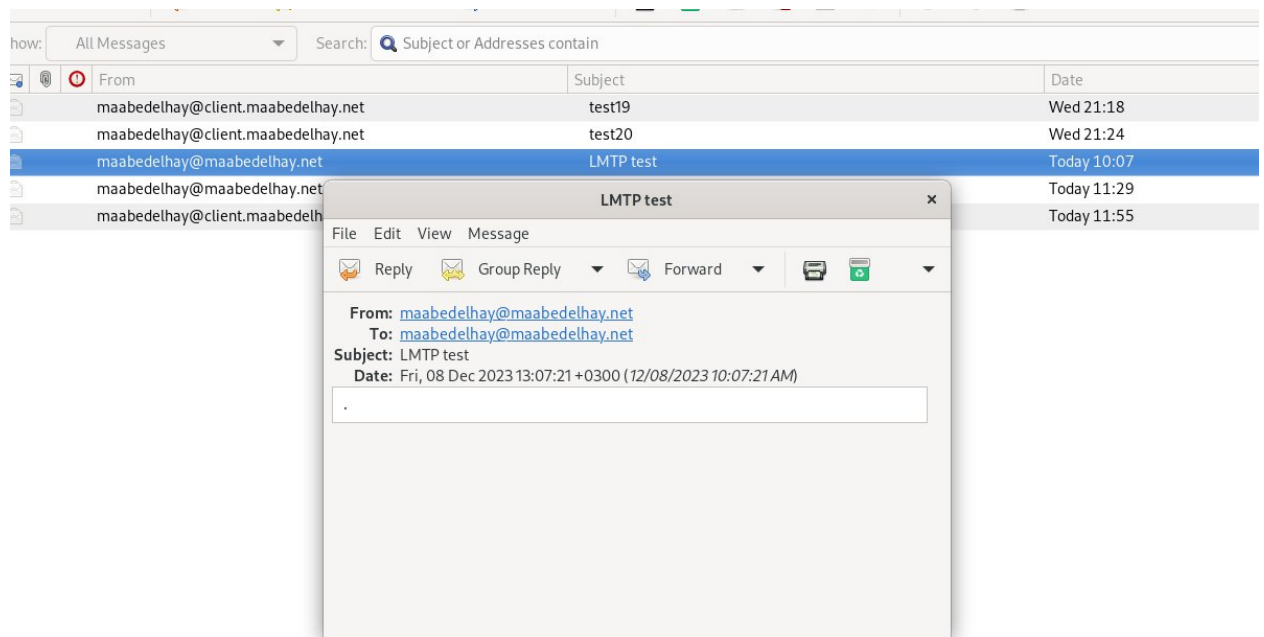
фигура 6 openssl



фигура 7 evolution

Я проверил, правильно ли отправляются сообщения электронной почты от клиента по электронной почте.

стандартный клиент Evolution, предварительно настроив настройки своего аккаунта, а именно для SMTP сервера указываем порт 587, STARTTLS и обычный пароль.



фигура 8 evolution

4. Вывод

Я научился настраивать SMTP-сервер с точки зрения настроек аутентификации.

5. Контрольные вопросы

1. Пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена:

```
auth_mechanisms = plain login
```

```
auth_username_format = %Ln
```

2. Почтовый Relay-сервер выполняет следующие функции:

- Пересылка почты: Relay-сервер получает почту от отправителя и пересылает ее адресату. Он действует как почтовый посредник между отправителем и получателем.
- Маршрутизация почты: Relay-сервер определяет наиболее эффективный маршрут для доставки почты на основе информации о доменах и MX-записях.
- Фильтрация спама и вредоносных писем: Relay-сервер может осуществлять проверку почты на наличие спама, вирусов и других вредоносных элементов перед ее передачей получателю.
- Контроль нагрузки: Relay-сервер может распределять нагрузку на несколько почтовых серверов для более эффективной обработки почты.

3. Некорректная настройка почтового сервера в качестве Relay-сервера может привести к следующим угрозам безопасности:

- Открытый ретранслятор: Если Relay-сервер настроен как открытый ретранслятор, злоумышленники могут использовать его для отправки спама или вредоносных писем без необходимости аутентификации.
- Ретрансляция спама: Если Relay-сервер позволяет отправителям ретранслировать почту через него без ограничений, он может стать центром распространения спама.

- Раскрытие информации: Некорректная настройка Relay-сервера может привести к раскрытию информации о доменах и получателях почты, что может быть использовано злоумышленниками для проведения атак или спам-кампаний.
- Недостаточная фильтрация: Если Relay-сервер не обеспечивает должную фильтрацию спама и вредоносных писем, получатель может быть подвержен атакам или нежелательной почте.
- Потеря контроля: Relay-сервер, настроенный неправильно, может потерять контроль над пересылкой почты, что может привести к нежелательным последствиям и нарушению безопасности