

Отчет по лабораторной работе № 10.  
Расширенные настройки SMTP-сервера

Данила Стариков  
НПИбд-02-22

2024

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Выполнение работы</b>	<b>4</b>
2.1	Настройка LMTP в Dovecote . . . . .	4
2.2	Настройка SMTP-аутентификации . . . . .	6
2.3	Настройка SMTP over TLS . . . . .	9
2.4	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	13
<b>3</b>	<b>Выводы</b>	<b>15</b>

# 1 Цель работы

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

## 2 Выполнение работы

### 2.1 Настройка LMTP в Dovecot

1. На виртуальной машине `server` вошли под пользователем и открыли терминал. Перешли в режим суперпользователя:

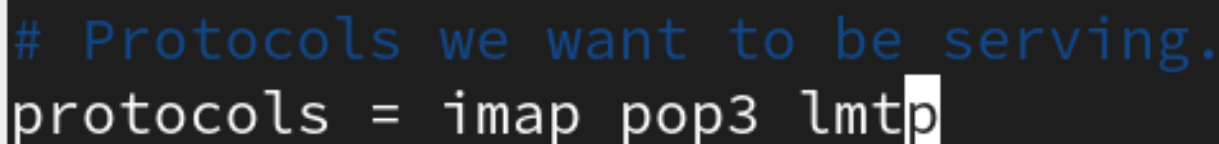
```
sudo -i
```

2. В дополнительном терминале запустили мониторинг работы почтовой службы:

```
sudo -i  
tail -f /var/log/maillog
```

3. Добавили в список протоколов, с которыми может работать Dovecot, протокол LMTP. Для этого в файле `/etc/dovecot/dovecot.conf` указали (Рис. 1)

```
protocols = imap pop3 lmtp
```



```
# Protocols we want to be serving.  
protocols = imap pop3 lmtp
```

Рис. 1: Обновление списка разрешенных протоколов в Dovecot.

4. Настроили в Dovecot сервис `lmtp` для связи с Postfix. Для этого в файле `/etc/dovecot/conf.d/10-master.conf` заменили определение сервиса `lmtp` на следующую запись (Рис. 2):

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



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

Рис. 2: Настройки сервера `lmtp`.

5. Переопределили в Postfix с помощью `postconf` передачу сообщений не на прямую, а через заданный unix-сокет:

```
postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'
```

6. В файле `/etc/dovecot/conf.d/10-auth.conf` задали формат имени пользователя для аутентификации в форме логина пользователя без указания домена (Рис. 3):

```
auth_username_format = %Ln
```

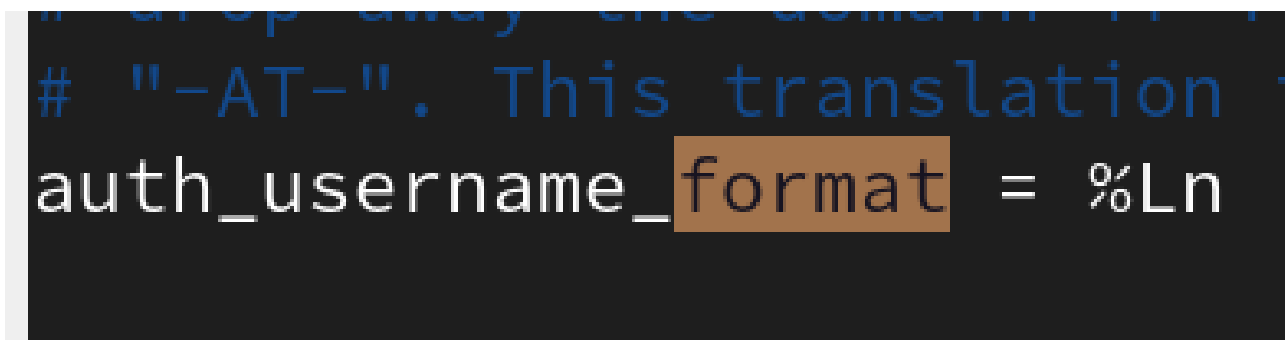


Рис. 3: Задание формата имени пользователя для аутентификации.

7. Перезапустите Postfix и Dovecot (Рис. 4):

```
systemctl restart postfix  
systemctl restart dovecot
```

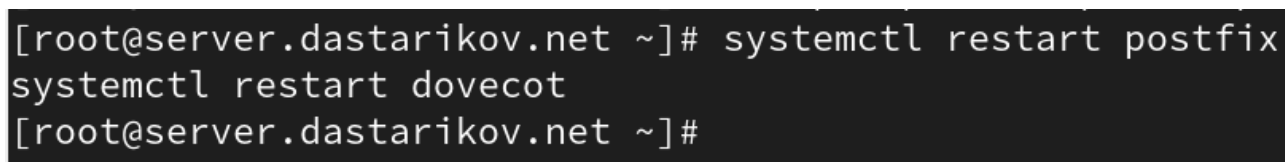


Рис. 4: Перезагрузка Postfix и Dovecot.

8. Из-под учётной записи своего пользователя отправили письмо с клиента:

```
echo . | mail -s "LMTP test" dastarikov@dastarikov.net
```

9. На сервере просмотрели почтовый ящик пользователя (Рис. 5 и 6):

```
MAIL=~/.Maildir/ mail
```

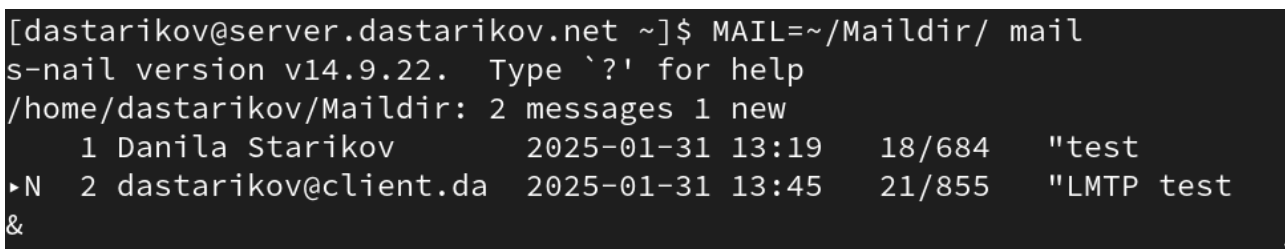


Рис. 5: Просмотр доставленного письма через утилиту `mail`.

```

Jan 31 13:45:45 client postfix/pickup[1062]: 6CA8450879: uid=1001 from=<dastarikov>
Jan 31 13:45:45 client postfix/cleanup[48996]: 6CA8450879: message-id=<20250131134545.6CA8450879@client.dastarikov.net>
Jan 31 13:45:45 client postfix/qmgr[1063]: 6CA8450879: from=<dastarikov@client.dastarikov.net>, size=346, nrcpt=1 (queue active)
Jan 31 13:45:45 client postfix/smtp[49002]: warning: run-time library vs. compile-time header version mismatch: OpenSSL 3.0.0 may not be compatible with OpenSSL 3.2.0
Jan 31 13:45:45 client postfix/smtp[49002]: 6CA8450879: to=<dastarikov@dastarikov.net>, relay=mail.dastarikov.net[192.168.1.1]:25, delay=0.31, delays=0.06/0.12/0.09/0.04, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as AEA2D10A9E1E)
Jan 31 13:45:45 server postfix/smtpd[47252]: warning: run-time library vs. compile-time header version mismatch: OpenSSL 3.0.0 may not be compatible with OpenSSL 3.2.0
Jan 31 13:45:45 server postfix/smtpd[47252]: connect from client.dastarikov.net[192.168.1.30]
Jan 31 13:45:45 server postfix/smtpd[47252]: AEA2D10A9E1E: client=client.dastarikov.net[192.168.1.30]
Jan 31 13:45:45 server postfix/cleanup[47256]: AEA2D10A9E1E: message-id=<20250131134545.6CA8450879@client.dastarikov.net>
Jan 31 13:45:45 server postfix/qmgr[47227]: AEA2D10A9E1E: from=<dastarikov@client.dastarikov.net>, size=561, nrcpt=1 (queue active)
Jan 31 13:45:45 server postfix/smtpd[47252]: disconnect from client.dastarikov.net[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Jan 31 13:45:45 server dovecot[47241]: lmtp(47259): Connect from local
Jan 31 13:45:45 server dovecot[47241]: lmtp(dastarikov)<47259><D8PeLQnUnGebuAAAAzqMKA>: msgid=<20250131134545.6CA8450879@client.dastarikov.net>; saved mail to INBOX
Jan 31 13:45:45 server postfix/lmtp[47258]: AEA2D10A9E1E: to=<dastarikov@dastarikov.net>, relay=server.dastarikov.net[private/dovecot-lmtp], delay=0.08, delays=0.02/0.01/0.03/0.01, dsn=2.0.0, status=sent (250 2.0.0 <dastarikov@dastarikov.net> D8PeLQnUnGebuAAAAzqMKA Saved)
Jan 31 13:45:45 server postfix/qmgr[47227]: AEA2D10A9E1E: removed
Jan 31 13:45:45 server dovecot[47241]: lmtp(47259): Disconnect from local: Logged out (state=READY)
Jan 31 13:45:45 client postfix/qmgr[1063]: 6CA8450879: removed

```

Рис. 6: Просмотр логов при отправке письма.

## 2.2 Настройка SMTP-аутентификации

1. В файле `/etc/dovecot/conf.d/10-master.conf` определили службу аутентификации пользователей (Рис. 7):

```

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

```

Рис. 7: Настройка службы аутентификации.

2. Для Postfix задали тип аутентификации SASL для `smtpd` и путь к соответствующему unix-сокету (Рис. 8):

```

postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'

```

```

[root@server.dastarikov.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'
[root@server.dastarikov.net ~]#

```

Рис. 8: Настройка типа аутентификации SASL для `smtpd`.

3. Настроили 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 спамрассылок (порядок указания опций имеет значение) (Рис. 9):

```

postconf -e 'smtpd_recipient_restrictions =
    ↪ reject_unknown_recipient_domain, permit_mynetworks,
    ↪ reject_non_fqdn_recipient, reject_unauth_destination,
    ↪ reject_unverified_recipient, permit'

```

```

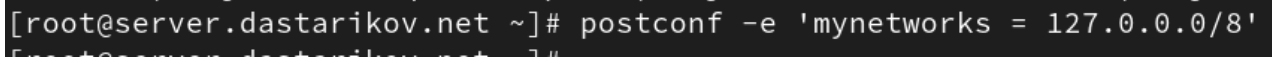
[root@server.dastarikov.net ~]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'

```

Рис. 9: Настройка Postfix для запрета спамрассылок.

4. В настройках Postfix ограничили приём почты только локальным адресом SMTP-сервера сети (Рис. 10):

```
postconf -e 'mynetworks = 127.0.0.0/8'
```



```
[root@server.dastarikov.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'
```

Рис. 10: Ограничение приема почты только локальным адресом.

5. Для проверки работы аутентификации временно запустили SMTP-сервер (порт 25) с возможностью аутентификации. Для этого в файле `/etc/postfix/master.cf` заменили строку

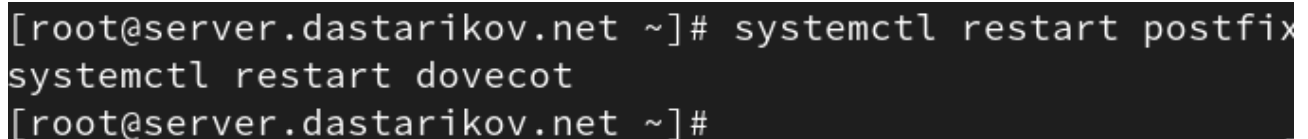
```
smtp inet n - n - - smtpd
```

на строку

```
smtp inet n - n - - smtpd
-o smtpd_sasl_auth_enable=yes
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient,
  ↪ reject_unknow, n_recipient_domain, permit_sasl_authenticated,
  ↪ reject
```

6. Перезапустили Postfix и Dovecot (Рис. 11):

```
systemctl restart postfix
systemctl restart dovecot
```



```
[root@server.dastarikov.net ~]# systemctl restart postfix
systemctl restart dovecot
[root@server.dastarikov.net ~]#
```

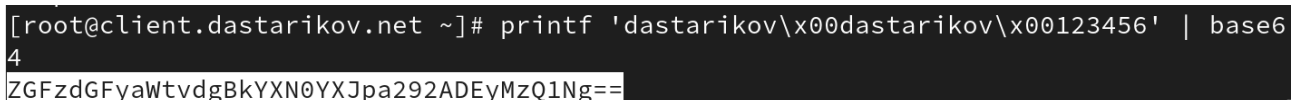
Рис. 11: Перезагрузка Postfix и Dovecot.

7. На клиенте установили telnet:

```
sudo -i
dnf -y install telnet
```

8. На клиенте получили строку для аутентификации (Рис. 12):

```
printf 'dastarikov\x00dastarikov\x00123456' | base64
```



```
[root@client.dastarikov.net ~]# printf 'dastarikov\x00dastarikov\x00123456' | base64
ZGFZdGFyaWtvdGkYXN0YXJpa292ADEyMzQ1Ng==
```

Рис. 12: Получение строки для аутентификации.

9. Подключились на клиенте к SMTP-серверу посредством telnet (Рис. 13):

```
telnet server.dastarikov.net 25
```

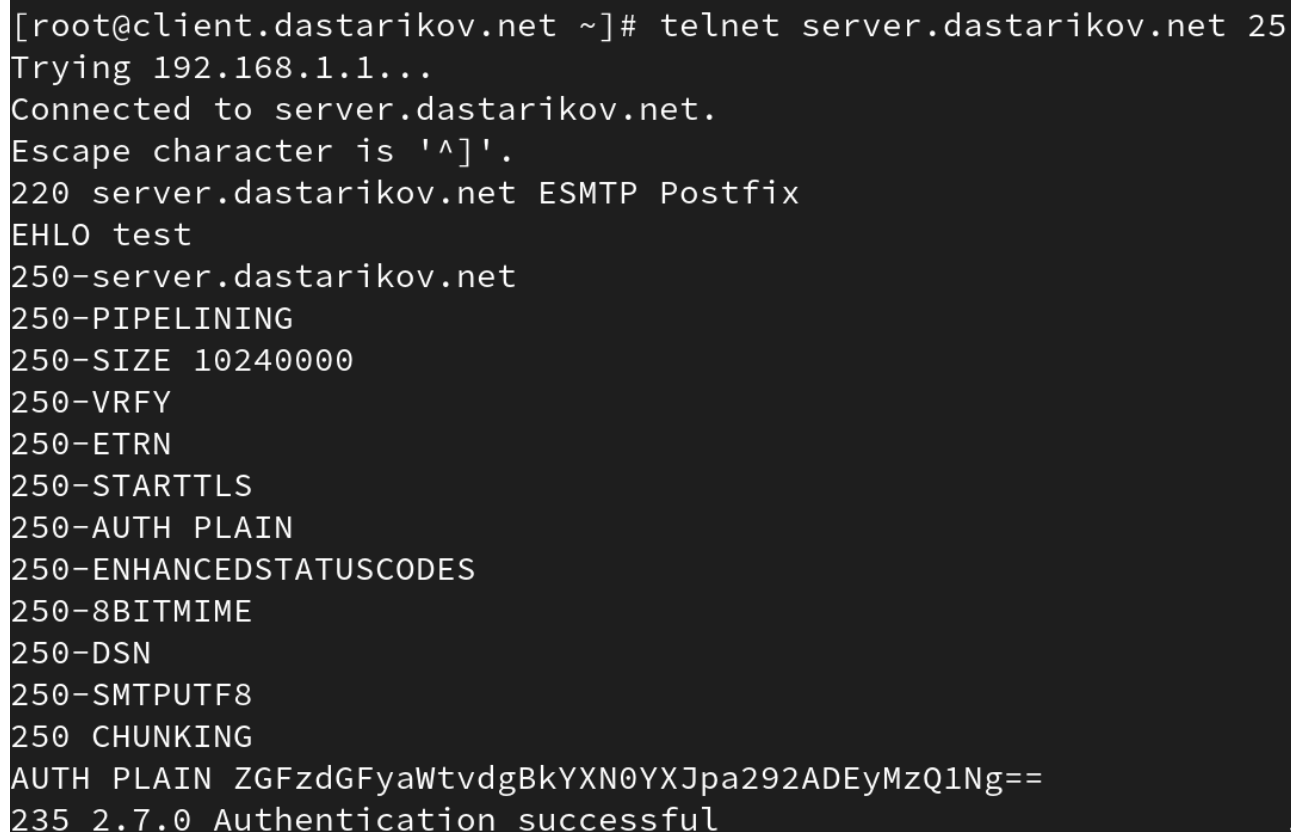


Протестировали соединение, введя

```
EHLO test
```

Проверили авторизацию, задав:

```
AUTH PLAIN <строка для аутентификации>
```

A screenshot of a terminal window with a black background and white text. The text shows a telnet session from a client to a server. The user enters 'telnet server.dastarikov.net 25' and the terminal shows the connection process, including the IP address 192.168.1.1... and the server's response '220 server.dastarikov.net ESMTP Postfix'. The user then enters 'EHLO test' and the server responds with a list of supported features: '250-server.dastarikov.net', '250-PIPELINING', '250-SIZE 10240000', '250-VRFY', '250-ETRN', '250-STARTTLS', '250-AUTH PLAIN', '250-ENHANCEDSTATUSCODES', '250-8BITMIME', '250-DSN', '250-SMTPUTF8', and '250 CHUNKING'. Finally, the user enters 'AUTH PLAIN ZGFzdGFyaWtvdgBkYXN0YXJpa292ADEyMzQ1Ng==' and the server responds with '235 2.7.0 Authentication successful'.

```
[root@client.dastarikov.net ~]# telnet server.dastarikov.net 25
Trying 192.168.1.1...
Connected to server.dastarikov.net.
Escape character is '^]'.
220 server.dastarikov.net ESMTP Postfix
EHLO test
250-server.dastarikov.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 ZGFzdGFyaWtvdgBkYXN0YXJpa292ADEyMzQ1Ng==
235 2.7.0 Authentication successful
```

Рис. 13: Подключение к SMTP-серверу через telnet.

Завершили сессию telnet на клиенте.

## 2.3 Настройка SMTP over TLS

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

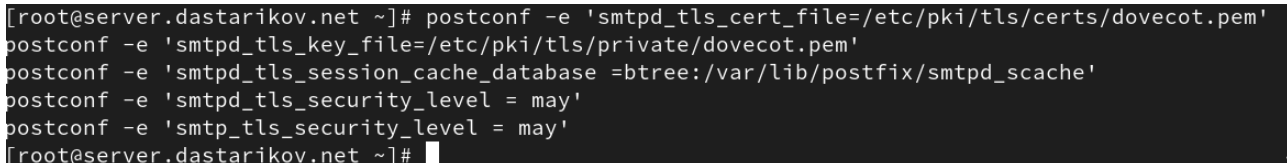
```
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
```

Сконфигурировали Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности (Рис. 14):

```

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'

```



```

[root@server.dastarikov.net ~]# 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'
[root@server.dastarikov.net ~]#

```

Рис. 14: Конфигурация Postfix для работы через TLS.

2. Для того чтобы запустить SMTP-сервер на 587-м порту, в файле `/etc/postfix/master.cf` заменили строки (Рис. 15)

```

smtp inet n - n - - smtpd
-o smtpd_sasl_auth_enable=yes
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient,
↳ reject_unknown, n_recipient_domain, permit_sasl_authenticated,
↳ reject

```

на следующую запись:

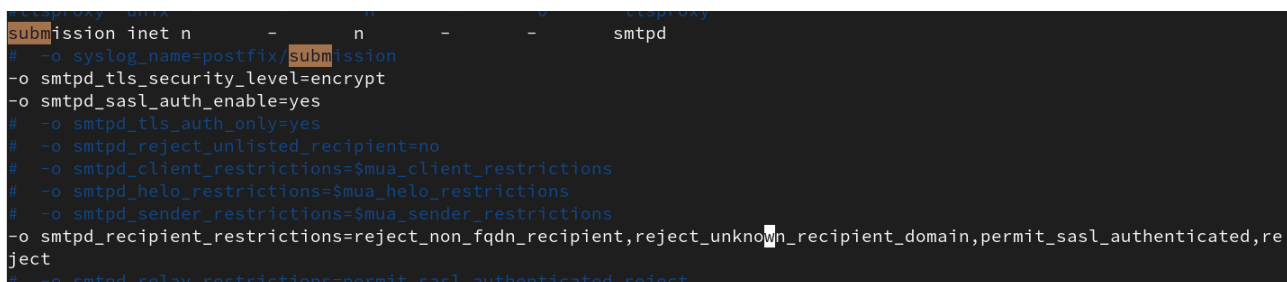
```
smtp inet n - n - - smtpd
```

и добавили следующие строки:

```

submission inet n - n - - smtpd
-o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_sasl_auth_enable=yes
-o smtpd_tls_auth_only=yes
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=$mua_client_restrictions
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient, reject_unknown, n_recipient_domain, permit_sasl_authenticated, re
ject
# -o smtpd_relay_restrictions=permit_sasl_authenticated, reject

```



```

# -o smtpd_relay_restrictions=permit_sasl_authenticated, reject
submission inet n - n - - smtpd
# -o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_sasl_auth_enable=yes
# -o smtpd_tls_auth_only=yes
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=$mua_client_restrictions
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient, reject_unknown, n_recipient_domain, permit_sasl_authenticated, re
ject
# -o smtpd_relay_restrictions=permit_sasl_authenticated, reject

```

Рис. 15: Изменение `/etc/postfix/master.cf`.

3. Настроили 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. Перезапустили Postfix:

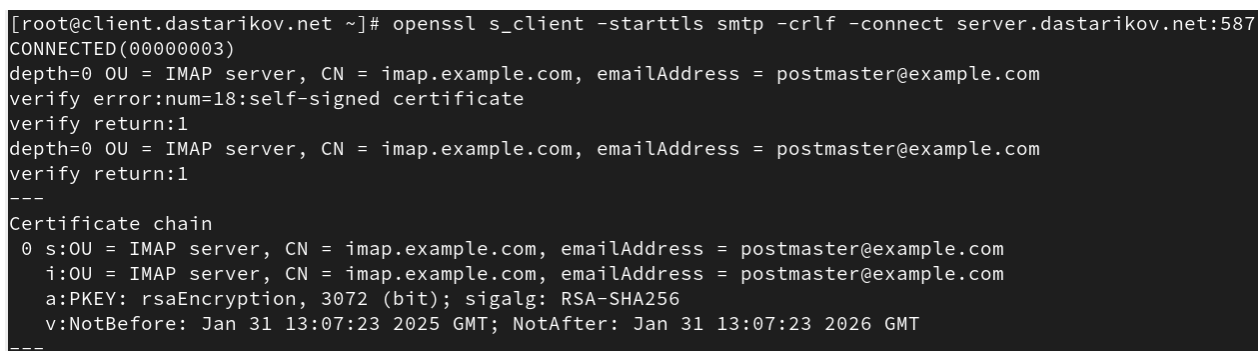
```
systemctl restart postfix
```

5. На клиенте подключились к SMTP-серверу через 587-й порт посредством `openssl` (вместо `dastarikov` используйте свой логин) (Рис. 16):

```

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

```



```

[root@client.dastarikov.net ~]# openssl s_client -starttls smtp -crlf -connect server.dastarikov.net:587
CONNECTED(00000003)
depth=0 OU = IMAP server, CN = imap.example.com, emailAddress = postmaster@example.com
verify error:num=18:self-signed certificate
verify return:1
depth=0 OU = IMAP server, CN = imap.example.com, emailAddress = postmaster@example.com
verify return:1
---
Certificate chain
 0 s:OU = IMAP server, CN = imap.example.com, emailAddress = postmaster@example.com
  i:OU = IMAP server, CN = imap.example.com, emailAddress = postmaster@example.com
  a:PKEY: rsaEncryption, 3072 (bit); sigalg: RSA-SHA256
  v:NotBefore: Jan 31 13:07:23 2025 GMT; NotAfter: Jan 31 13:07:23 2026 GMT
---

```

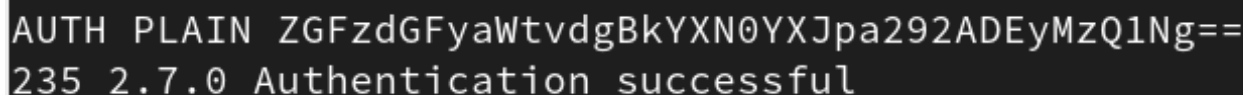
Рис. 16: Подключение к SMTP-серверу через `openssl`.

Протестировали подключение по `telnet` (Рис. 17):

```
EHLO test
```

Проверили аутентификацию (Рис. 17):

```
AUTH PLAIN <строка для аутентификации>
```



```

AUTH PLAIN ZGFzdGFyaWtvdgBkYXN0YXJpa292ADEyMzQ1Ng==
235 2.7.0 Authentication successful

```

Рис. 17: Проверка подключения к SMTP-серверу через `telnet`.

6. Проверили корректность отправки почтовых сообщений с клиента посредством почтового клиента Evolution, предварительно скорректировав настройки учётной записи, а именно для SMTP-сервера указали порт 587, STARTTLS и обычный пароль (Рис. 18-20).

**Account Editor** [X]

Identity  
Receiving Email  
Receiving Options  
**Sending Email**  
Defaults  
Composing Messages  
Security

Server Type: **SMTP**  
Description: For delivering mail by connecting to a remote mailhub using SMTP.

---

**Configuration**  
Server:  Port:  [v]  
☒ Server requires authentication

**Security**  
Encryption method:  [v]

**Authentication**  
Type:   [v]  
Username:

[Cancel] [OK]

Рис. 18: Корректировка почтового клиента Evolution.

**Mail authentication request** [X]

**Mail authentication request**  
Please enter the password for mail transport "dastarikov@dastarikov.net : dastarikov@dastarikov.net".  
(host: mail.dastarikov.net)

User Name:

Password:

☒ Add this password to your keyring

[Cancel] [OK]

Рис. 19: Аутентификация пользователя при попытке отправить письмо.

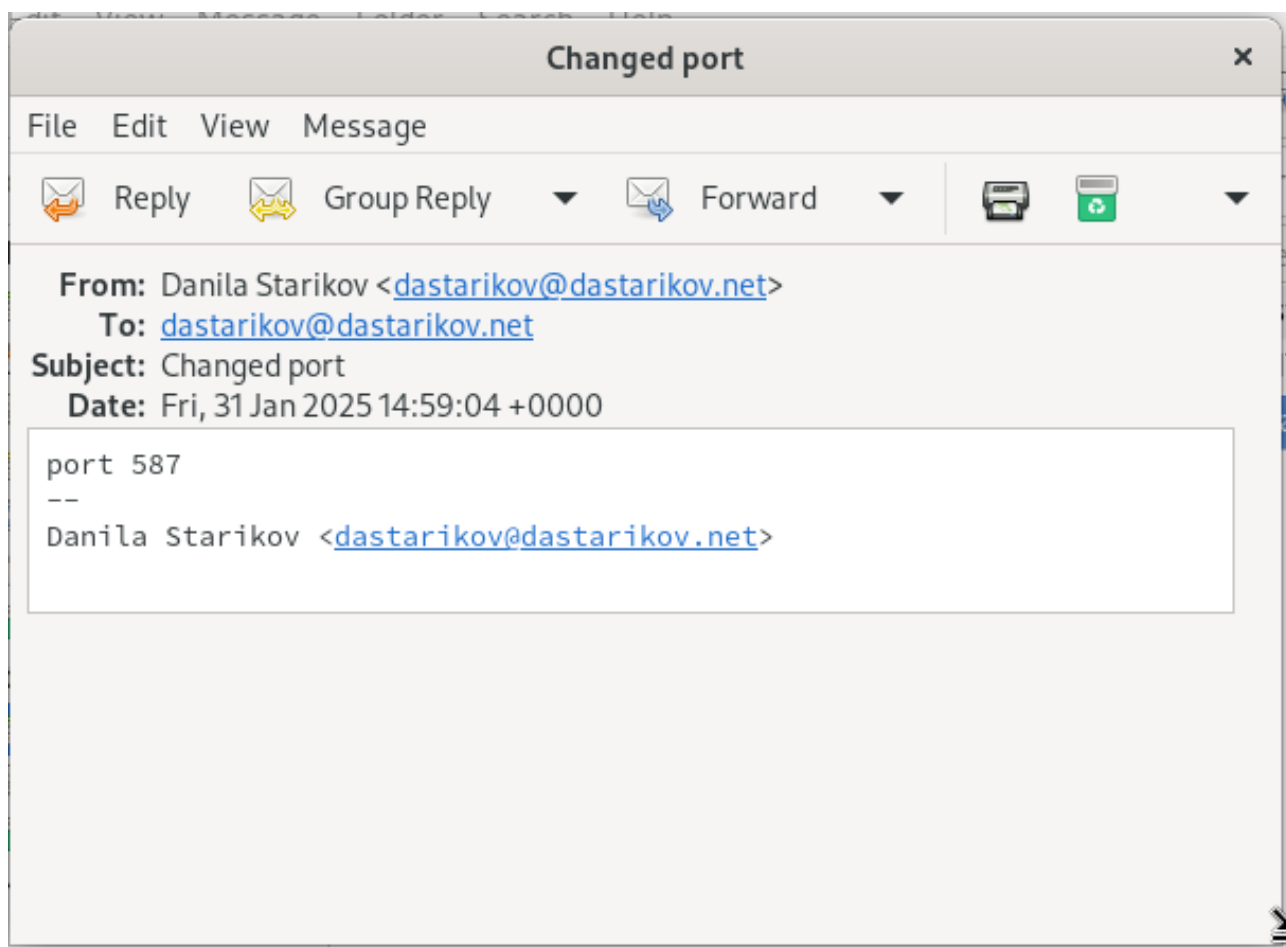


Рис. 20: Просмотр пришедшего письма.

## 2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине **server** перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`. В соответствующие подкаталоги поместили конфигурационные файлы Dovecot и Postfix:

```
cd /vagrant/provision/server
cp -R /etc/dovecot/dovecot.conf
  ↳ /vagrant/provision/server/mail/etc/dovecot/
cp -R /etc/dovecot/conf.d/10-master.conf
  ↳ /vagrant/provision/server/mail/etc/dovecot/conf.d/
cp -R /etc/dovecot/conf.d/10-auth.conf
  ↳ /vagrant/provision/server/mail/etc/dovecot/conf.d/
mkdir -p /vagrant/provision/server/mail/etc/postfix/
cp -R /etc/postfix/master.cf
  ↳ /vagrant/provision/server/mail/etc/postfix/
```

2. Внесли соответствующие изменения по расширенной конфигурации SMTP-сервера в файл `/vagrant/provision/server/mail.sh`:

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install postfix
dnf -y install dovecot
dnf -y install telnet
echo "Copy configuration files"
cp -R /vagrant/provision/server/mail/etc/* /etc
chown -R root:root /etc/postfix
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-service smtp --permanent
firewall-cmd --add-service pop3 --permanent
firewall-cmd --add-service pop3s --permanent
firewall-cmd --add-service imap --permanent
firewall-cmd --add-service imaps --permanent
firewall-cmd --add-service smtp-submission --permanent
firewall-cmd --reload
echo "Start postfix service"
systemctl enable postfix
systemctl start postfix
echo "Configure postfix"
postconf -e 'mydomain = dastarikov.net'
postconf -e 'myorigin = $mydomain'
postconf -e 'inet_protocols = ipv4'
postconf -e 'inet_interfaces = all'
postconf -e 'mydestination = $myhostname, localhost.$mydomain,
↳ localhost, $mydomain'
#postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'
echo "Configure postfix for dovecot"
postconf -e 'home_mailbox = Maildir/'
echo "Configure postfix for auth"
postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'
postconf -e 'smtpd_recipient_restrictions =
↳ reject_unknown_recipient_domain, permit_mynetworks,
↳ reject_non_fqdn_recipient, reject_unauth_destination,
↳ reject_unverified_recipient, permit'

postconf -e 'mynetworks = 127.0.0.0/8'
echo "Configure postfix for SMTP over TLS"
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
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'  
postfix set-permissions  
restorecon -vR /etc  
systemctl stop postfix  
systemctl start postfix  
systemctl restart dovecot
```

3. Внесли изменения в файл `/vagrant/provision/client/mail.sh`, добавив установку Telnet.

```
dnf -y install telnet
```

### 3 Выводы

В результате выполнения лабораторной работы приобрели практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.