

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ
ПАТРИСА ЛУМУМБЫ**

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

**ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 10**

Дисциплина «Администрирование сетевых подсистем»

Тема «Расширенные настройки SMTP-сервера»

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

МОСКВА

2023 г.

Цель работы

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

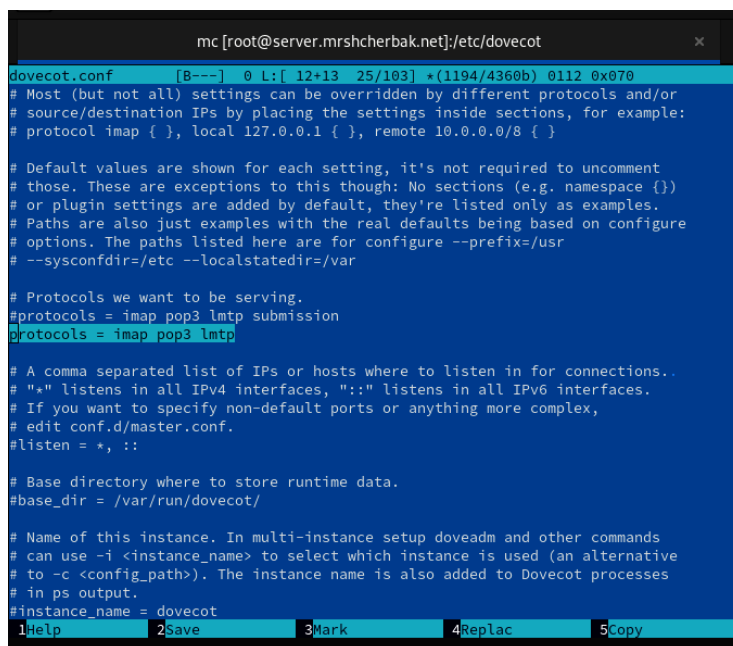
Задание

1. Настроить Dovecot для работы с LMTP.
2. Настроить аутентификацию посредством SASL на SMTP-сервере.
3. Настроить работу SMTP-сервера поверх TLS.
4. Скорректировать скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server.

Выполнение

1. Настройка LMTP в Dovecot

1. На виртуальной машине server вошла под своим пользователем и открыла терминал. Перешла в режим суперпользователя. В дополнительном терминале запустила мониторинг работы почтовой службы.
2. Добавила в список протоколов, с которыми может работать Dovecot, протокол LMTP (рис.1.1).



```
mc [root@server.mrshcherbak.net]:/etc/dovecot
dovecot.conf [B---] 0 L: [ 12+13 25/103] *(1194/4360b) 0112 0x070
# Most (but not all) settings can be overridden by different protocols and/or
# source/destination IPs by placing the settings inside sections, for example:
# protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }

# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

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

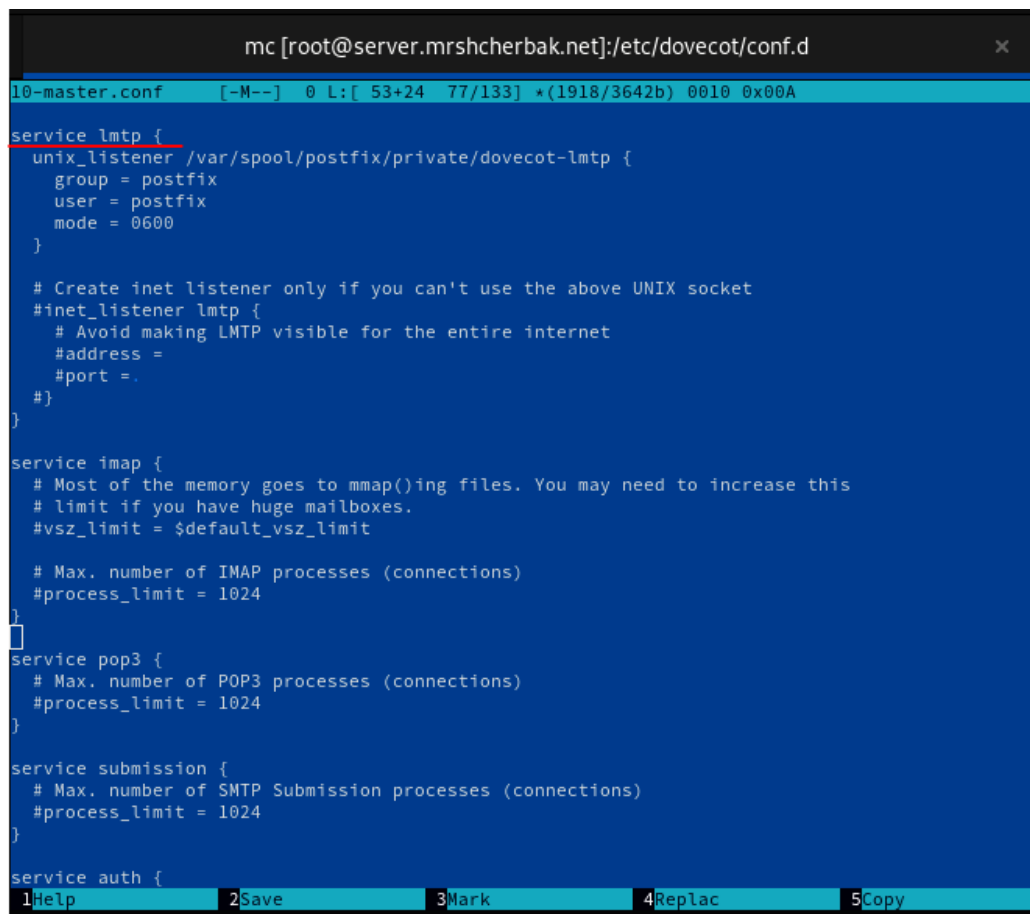
# A comma separated list of IPs or hosts where to listen in for connections..
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
#listen = *, ::

# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Name of this instance. In multi-instance setup doveadm and other commands
# can use -i <instance_name> to select which instance is used (an alternative
# to -c <config_path>). The instance name is also added to Dovecot processes
# in ps output.
#instance_name = dovecot
1Help 2Save 3Mark 4Replac 5Copy
```

Рис.1.1. Редактирование файла /etc/dovecot/dovecot.conf

3. Настроила в Dovecot сервис lmtp для связи с Postfix. Для этого в файле /etc/dovecot/conf.d/10-master.conf заменила определение сервиса lmtp на запись, представленную на рис.1.2. Эта запись определяет расположение файла с описанием прослушиваемого unix-сокета, а также задаёт права доступа к нему и определяет принадлежность к группе и пользователю postfix.



```
mc [root@server.mrshcherbak.net]:/etc/dovecot/conf.d
10-master.conf [-M--] 0 L: [ 53+24 77/133] *(1918/3642b) 0010 0x00A
service lmtp {
    unix_listener /var/spool/postfix/private/dovecot-lmtp {
        group = postfix
        user = postfix
        mode = 0600
    }

    # Create inet listener only if you can't use the above UNIX socket
    #inet_listener lmtp {
        # Avoid making LMTP visible for the entire internet
        #address =
        #port =
    #}
}

service imap {
    # Most of the memory goes to mmap()ing files. You may need to increase this
    # limit if you have huge mailboxes.
    #vsz_limit = $default_vsz_limit

    # Max. number of IMAP processes (connections)
    #process_limit = 1024
}

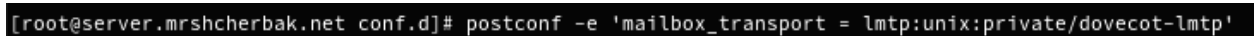
service pop3 {
    # Max. number of POP3 processes (connections)
    #process_limit = 1024
}

service submission {
    # Max. number of SMTP Submission processes (connections)
    #process_limit = 1024
}

service auth {
1Help      2Save      3Mark      4Replac    5Copy
```

Рис.1.2. Настройка в Dovecot сервиса lmtp для связи с Postfix

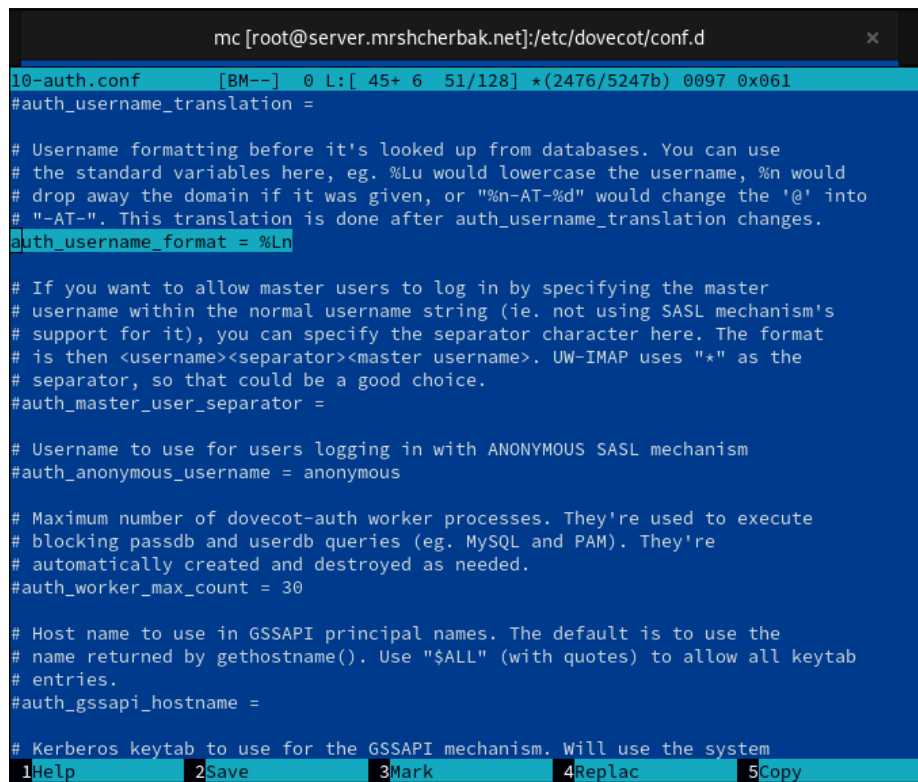
4. Переопределила в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-соклет (рис.1.3).



```
[root@server.mrshcherbak.net conf.d]# postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'
```

Рис.1.3. Выполнение команды

5. В файле /etc/dovecot/conf.d/10-auth.conf задала формат имени пользователя для аутентификации в форме логина пользователя без указания домена (рис.1.4).



```
mc [root@server.mrshcherbak.net]:/etc/dovecot/conf.d
10-auth.conf [BM--] 0 L: [ 45+ 6 51/128] *(2476/5247b) 0097 0x061
#auth_username_translation =

# Username formatting before it's looked up from databases. You can use
# the standard variables here, eg. %Lu would lowercase the username, %n would
# drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
# "-AT-". This translation is done after auth_username_translation changes.
auth_username_format = %Ln

# If you want to allow master users to log in by specifying the master
# username within the normal username string (ie. not using SASL mechanism's
# support for it), you can specify the separator character here. The format
# is then <username><separator><master username>. UW-IMAP uses "*" as the
# separator, so that could be a good choice.
#auth_master_user_separator =

# Username to use for users logging in with ANONYMOUS SASL mechanism
#auth_anonymous_username = anonymous

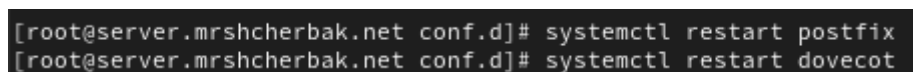
# Maximum number of dovecot-auth worker processes. They're used to execute
# blocking passdb and userdb queries (eg. MySQL and PAM). They're
# automatically created and destroyed as needed.
#auth_worker_max_count = 30

# Host name to use in GSSAPI principal names. The default is to use the
# name returned by gethostname(). Use "$ALL" (with quotes) to allow all keytab
# entries.
#auth_gssapi_hostname =

# Kerberos keytab to use for the GSSAPI mechanism. Will use the system
1Help 2Save 3Mark 4Replac 5Copy
```

Рис.1.4. Редактирование файла /etc/dovecot/conf.d/10-auth.conf

6. Перезапустила Postfix и Dovecot (рис.1.5).



```
[root@server.mrshcherbak.net conf.d]# systemctl restart postfix
[root@server.mrshcherbak.net conf.d]# systemctl restart dovecot
```

Рис.1.5. Выполнение команд

7. Из-под учётной записи своего пользователя отправила письмо с клиента (рис.1.6).

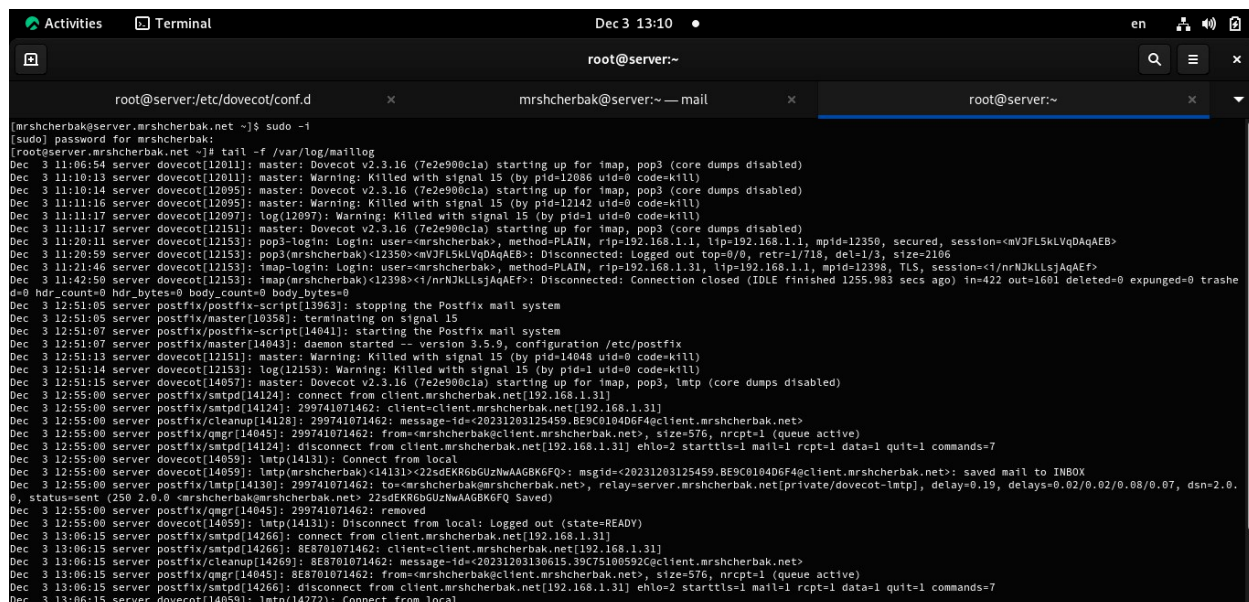


```
[mrshcherbak@client.mrshcherbak.net ~]$. echo . | mail -s "LMTP test" mrshcherbak@mrshcherbak.net
```

Рис.1.6. Отправка письма с клиента

Просмотрела логи при мониторинге почтовой службы (рис.1.6). Пользователь mrshcherbak устанавливает соединение с почтовым сервером через SMTP. Почтовый сервер принимает запрос от клиента mrshcherbak.net с IP-адресом 192.168.1.31, начинает обработку сообщения с идентификатором 20231203125459 от отправителя mrshcherbak. Сообщение добавляется в очередь для последующей обработки. Почтовый сервер закрывает соединение с клиентом после завершения этапа принятия данных. Dovecot, сервер для обработки входящей почты, устанавливает соединение для обработки сообщения. Dovecot получает и

обрабатывает сообщение для пользователя mrshcherbak. Почтовый сервер передает сообщение Dovecot для доставки пользователю mrshcherbak через протокол IMAP. Успешное сохранение сообщения в почтовом ящике пользователя mrshcherbak. Удаление сообщения из очереди после успешной обработки.



```
root@server:/etc/dovecot/conf.d
mrshcherbak@server:~ — mail
root@server:~

[mrshcherbak@server mrshcherbak.net ~]$ sudo -i
[sudo] password for mrshcherbak:
[root@server mrshcherbak.net ~]# tail -f /var/log/maillog
Dec 3 11:06:54 server dovecot[12011]: master: Dovecot v2.3.16 (7e2e900c1a) starting up for imap, pop3 (core dumps disabled)
Dec 3 11:10:13 server dovecot[12011]: master: Warning: Killed with signal 15 (by pid=12086 uid=0 code=kill)
Dec 3 11:10:14 server dovecot[12095]: master: Dovecot v2.3.16 (7e2e900c1a) starting up for imap, pop3 (core dumps disabled)
Dec 3 11:11:16 server dovecot[12095]: master: Warning: Killed with signal 15 (by pid=12142 uid=0 code=kill)
Dec 3 11:11:17 server dovecot[12097]: log(12097): Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Dec 3 11:11:17 server dovecot[12153]: master: Dovecot v2.3.16 (7e2e900c1a) starting up for imap, pop3 (core dumps disabled)
Dec 3 11:20:11 server dovecot[12153]: pop3-login: Login: user=<mrshcherbak>, method=PLAIN, rip=192.168.1.1, lip=192.168.1.1, mpid=12350, secured, session=<mVJfLSkLVQdAqAE>
Dec 3 11:20:59 server dovecot[12153]: pop3(mrshcherbak)<12350><mVJfLSkLVQdAqAE>: Disconnected: Logged out top=0/0, retr=1/718, del=1/3, size=2106
Dec 3 11:42:58 server dovecot[12153]: imap-login: Login: user=<mrshcherbak>, method=PLAIN, rip=192.168.1.31, lip=192.168.1.1, mpid=12398, TLS, session=<1/nrNJKLLsJAqAE>
Dec 3 11:42:58 server dovecot[12153]: imap(mrshcherbak)<12398><1/nrNJKLLsJAqAE>: Disconnected: Connection closed (IDLE finished 1255.983 secs ago) in=422 out=1601 deleted=0 expunged=0 trash=0
Dec 3 12:51:05 server postfix/master[10350]: terminating on signal 15
Dec 3 12:51:07 server postfix/postfix-script[14041]: starting the Postfix mail system
Dec 3 12:51:07 server postfix/master[14043]: daemon started -- version 3.5.9, configuration /etc/postfix
Dec 3 12:51:12 server dovecot[12153]: master: Warning: Killed with signal 15 (by pid=14048 uid=0 code=kill)
Dec 3 12:51:14 server dovecot[12153]: log(12153): Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Dec 3 12:51:15 server dovecot[14057]: master: Dovecot v2.3.16 (7e2e900c1a) starting up for imap, pop3, lmtp (core dumps disabled)
Dec 3 12:55:00 server postfix/smtpd[14124]: connect from client.mrshcherbak.net[192.168.1.31]
Dec 3 12:55:00 server postfix/smtpd[14124]: 299741071462: client=client.mrshcherbak.net[192.168.1.31]
Dec 3 12:55:00 server postfix/cleanup[14126]: 299741071462: message-id=<20231203125459.BE9C010406F4qclient.mrshcherbak.net>
Dec 3 12:55:00 server postfix/qmgr[14045]: 299741071462: from=<mrshcherbak@client.mrshcherbak.net>, size=576, nrcpt=1 (queue active)
Dec 3 12:55:00 server postfix/smtpd[14124]: disconnect from client.mrshcherbak.net[192.168.1.31] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Dec 3 12:55:00 server postfix/lmtp[14131]: Connect from local
Dec 3 12:55:00 server dovecot[14059]: lmtp(mrshcherbak)<14131><22sdEKRB6GzNwAGBK6FQ>: msgid=<20231203125459.BE9C010406F4qclient.mrshcherbak.net>; saved mail to INBOX
Dec 3 12:55:00 server postfix/lmtp[14130]: 299741071462: to=<mrshcherbak@mrshcherbak.net>, relay=server.mrshcherbak.net[private/dovecot-lmtp], delay=0.19, delays=0.02/0.02/0.08/0.07, dsn=2.0.0, status=sent (250 2.0.0 <mrshcherbak@mrshcherbak.net> 22sdEKRB6GzNwAGBK6FQ Saved)
Dec 3 12:55:00 server postfix/qmgr[14045]: 299741071462: removed
Dec 3 12:55:00 server dovecot[14059]: lmtp(14131): Disconnect from local: Logged out (state=READY)
Dec 3 13:06:15 server postfix/smtpd[14266]: connect from client.mrshcherbak.net[192.168.1.31]
Dec 3 13:06:15 server postfix/smtpd[14266]: 8E8701071462: client=client.mrshcherbak.net[192.168.1.31]
Dec 3 13:06:15 server postfix/cleanup[14269]: 8E8701071462: message-id=<20231203130615.39C75100592Cqclient.mrshcherbak.net>
Dec 3 13:06:15 server postfix/qmgr[14045]: 8E8701071462: from=<mrshcherbak@client.mrshcherbak.net>, size=576, nrcpt=1 (queue active)
Dec 3 13:06:15 server postfix/smtpd[14266]: disconnect from client.mrshcherbak.net[192.168.1.31] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Dec 3 13:06:15 server dovecot[14059]: lmtp(14272): Connect from local
```

Рис.1.6. Мониторинг почтовой службы

Доставка сообщений в почтовый ящик (почтового клиента) (рис.1.7).

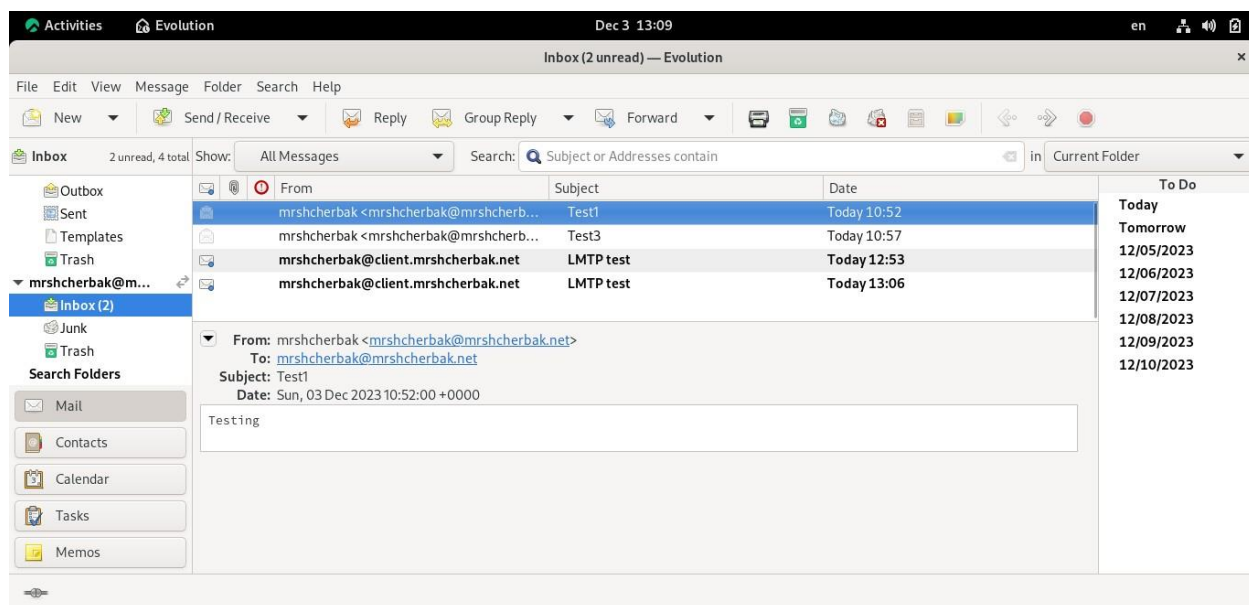
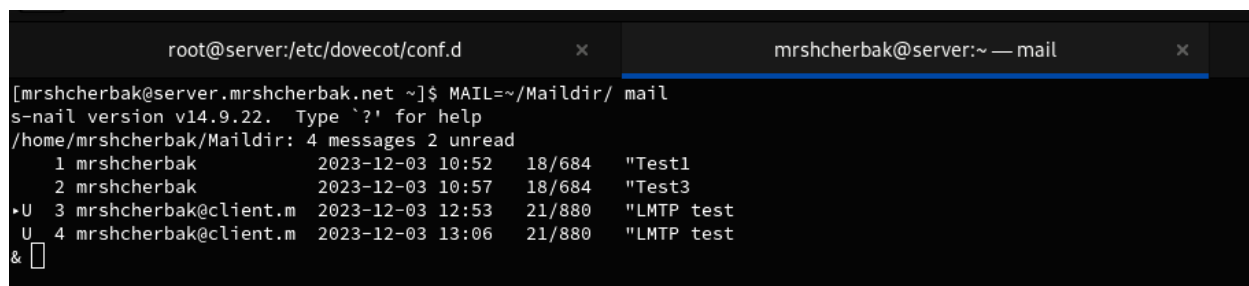


Рис.1.7. Проверка доставки писем

8. На сервере просмотрела почтовый ящик пользователя и убедилась, что отправленное с клиента письмо доставлено в почтовый ящик на сервере (рис.1.8).



```
root@server:/etc/dovecot/conf.d x mrshcherbak@server:~ — mail x
[mrshcherbak@server.mrshcherbak.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/mrshcherbak/Maildir: 4 messages 2 unread
 1 mrshcherbak      2023-12-03 10:52   18/684   "Test1
 2 mrshcherbak      2023-12-03 10:57   18/684   "Test3
•U 3 mrshcherbak@client.m 2023-12-03 12:53   21/880   "LMTP test
  U 4 mrshcherbak@client.m 2023-12-03 13:06   21/880   "LMTP test
& 
```

Рис.1.8. Проверка доставки писем

2. Настройка SMTP-аутентификации

1. В файле `/etc/dovecot/conf.d/10-master.conf` определила службу аутентификации пользователей (рис.2.1).

Фрагмент конфигурации в файле настраивает службу аутентификации пользователей.

`service auth`: начало блока конфигурации службы аутентификации.

`Unix_Listener /var/spool/postfix/private/auth` : определение Unix сокета для службы аутентификации, используемого Postfix.

`group = postfix`: группа, к которой принадлежит сокет.


`User = postfix`: пользователь, которому принадлежит сокет.

`mode = 0660`: режим доступа к сокету.

`unix_listener auth-userdb`: определение Unix сокета для процесса аутентификации пользователей.

`mode = 0600`: режим доступа к сокету аутентификации пользователей.

`user = dovecot`: пользователь, которому принадлежит сокет аутентификации пользователей.



```
mc [root@server.mrshcherbak.net]:/etc/dovecot/conf.d x mrs
/etc/dovecot/conf.d/10-master.conf
service auth {
# auth_socket_path points to this userdb socket by default. It's typically
# used by dovecot-lda, doveadm, possibly imap process, etc. Users that have
# full permissions to this socket are able to get a list of all usernames and
# get the results of everyone's userdb lookups.
#
# The default 0666 mode allows anyone to connect to the socket, but the
# userdb lookups will succeed only if the userdb returns an "uid" field that
# matches the caller process's UID. Also if caller's uid or gid matches the
# 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 /var/spool/postfix/private/auth {
    group = postfix
    user = postfix
    mode = 0660
}

# Postfix smtp-auth
unix_listener auth-userdb {
    mode = 0600
    user = dovecot
}

# Auth process is run as this user.
#user = $default_internal_user
}

service auth-worker {
# Auth worker process is run as root by default, so that it can access
# /etc/shadow. If this isn't necessary, the user should be changed to
# $default_internal_user.
#user = root
}
```

Рис.2.1. Содержимое файла /etc/dovecot/conf.d/10-master.conf

2. Для Postfix задала тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету, а также настроила Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины, обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок. В настройках Postfix ограничила приём почты только локальным адресом SMTP-сервера сети. Действия представлены на рис.2.2.

- `postconf -e 'smtpd_sasl_type = dovecot':` команда устанавливает тип аутентификации SASL для smtpd в значение "dovecot". Таким образом, Postfix будет использовать Dovecot для аутентификации пользователей.
- `postconf -e 'smtpd_sasl_path = private/auth':` устанавливает путь к unix-сокету для аутентификации SASL. Значение "private/auth" указывает на сокет, используемый Dovecot для аутентификации.
- `postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain,`

permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit': здесь настроены ограничения для приема почты. Каждый параметр разделенный запятой представляет собой различные правила:

- reject_unknown_recipient_domain: отклоняет почту с неизвестным доменом получателя.
 - permit_mynetworks: разрешает отправку почты от клиентов в локальной сети, указанной в mynetworks.
 - reject_non_fqdn_recipient: отклоняет почту, если домен получателя не является полностью доменным именем.
 - reject_unauth_destination: отклоняет почту с неподтвержденным адресом назначения.
 - reject_unverified_recipient: отклоняет почту с неподтвержденным получателем.
 - permit: разрешает все остальные случаи.
- postconf -e 'mynetworks = 127.0.0.0/8': команда определяет список сетей (mynetworks), которые считаются локальными. В данном случае, указана сеть 127.0.0.0/8, что включает в себя все IP-адреса в диапазоне от 127.0.0.1 до 127.255.255.255. Это позволяет ограничить прием почты только из локальной сети.

```
[root@server.mrshcherbak.net conf.d]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.mrshcherbak.net conf.d]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.mrshcherbak.net conf.d]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'
[root@server.mrshcherbak.net conf.d]# postconf -e 'mynetworks = 127.0.0.0/8'
[root@server.mrshcherbak.net conf.d]#
```

Рис.2.2. Выполнение команд

3. Для проверки работы аутентификации временно запустила SMTP-сервер (порт 25) с возможностью аутентификации. Для этого в файл /etc/postfix/master.cf внесла изменения (рис.2.3).

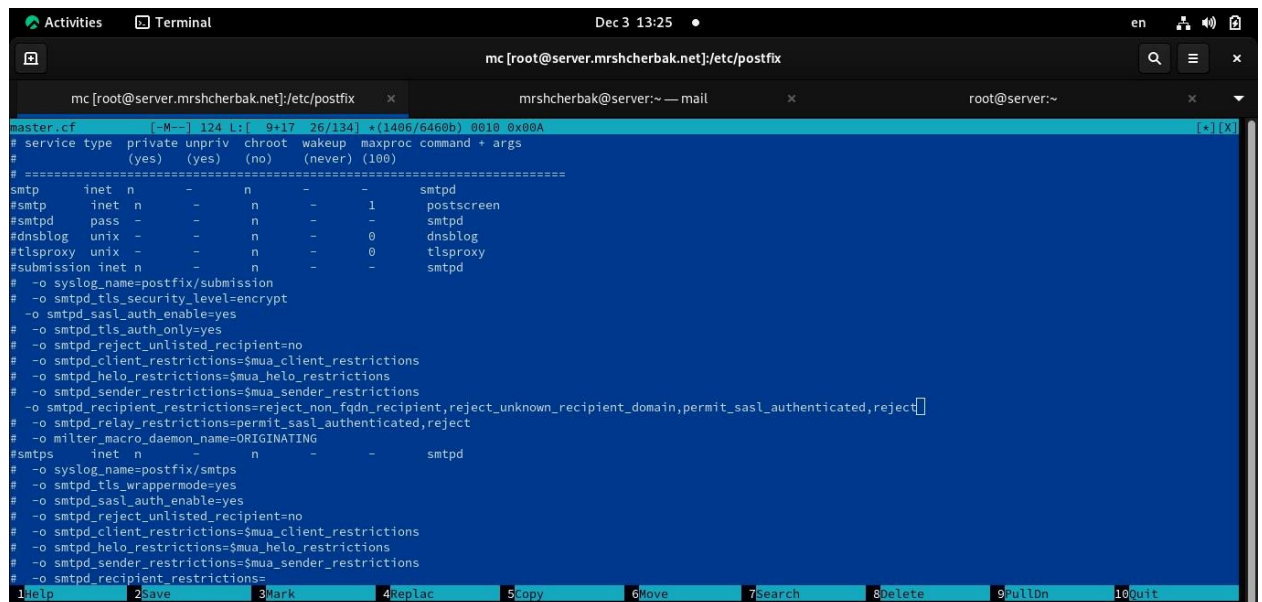


Рис.2.3. Редактирование файла /etc/postfix/master.cf

4. Перезапустила Postfix и Dovecot (рис.2.4).

```
[root@server.mrshcherbak.net conf.d]# systemctl restart postfix
[root@server.mrshcherbak.net conf.d]# systemctl restart dovecot
```

Рис.2.4. Выполнение команд

5. На клиенте установила telnet (рис.2.5).

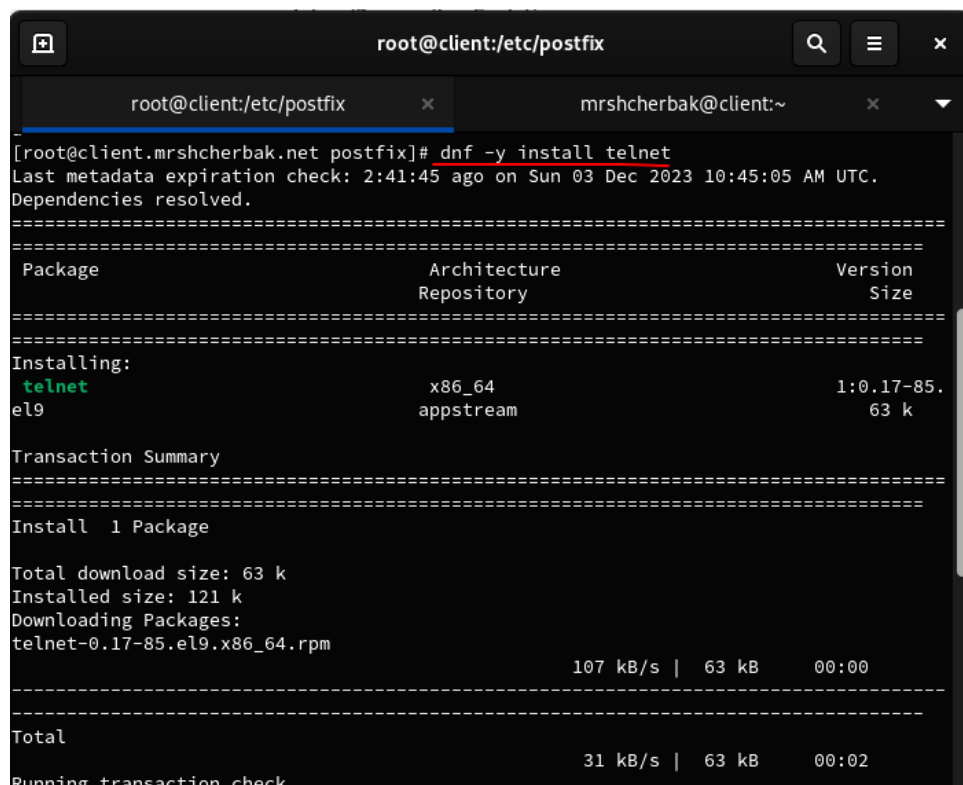


Рис.2.5. Установка telnet

6. На клиенте получила строку для аутентификации, подключилась к SMTP-серверу посредством telnet и протестировала соединение, введя EHLO test. Проверила авторизацию и завершила сессию. Действия представлены на рис.2.6.

```
[root@client.mrshcherbak.net postfix]# printf 'mrshcherbak\x00mrshcherbak\x00Rastamana035' | base64
bXJzaGNoZXJiYW5AbXJzaGNoZXJiYW5AUmFzdGFtYW5hMDM1
[root@client.mrshcherbak.net postfix]# telnet server.mrshcherbak.net 25
Trying 192.168.1.1...
Connected to server.mrshcherbak.net.
Escape character is '^]'.
220 server.mrshcherbak.net ESMTS Postfix
EHLO test
250-server.mrshcherbak.net
250-PIPELINING
250-SIZE 10240000
250-VRFB
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN bXJzaGNoZXJiYW5AbXJzaGNoZXJiYW5AUmFzdGFtYW5hMDM1
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
Connection closed by foreign host.
[root@client.mrshcherbak.net postfix]#
```

Рис.2.6. Выполнение команд

3. Настройка SMTP over TLS

1. Настроила на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно скопировала необходимые файлы сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги. Сконфигурировала Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности. Действия представлены на рис.3.1.

```
[root@server.mrshcherbak.net ~]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
[root@server.mrshcherbak.net ~]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
[root@server.mrshcherbak.net ~]# postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
[root@server.mrshcherbak.net ~]# postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
[root@server.mrshcherbak.net ~]# postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
[root@server.mrshcherbak.net ~]# postconf -e 'smtpd_tls_security_level = may'
[root@server.mrshcherbak.net ~]# postconf -e 'smtpd_tls_security_level = may'
[root@server.mrshcherbak.net ~]#
```

Рис.3.1. Выполнение команд

2. Для того чтобы запустить SMTP-сервер на 587-м порту, в файл /etc/postfix/master.cf внесла изменения (рис.3.2).

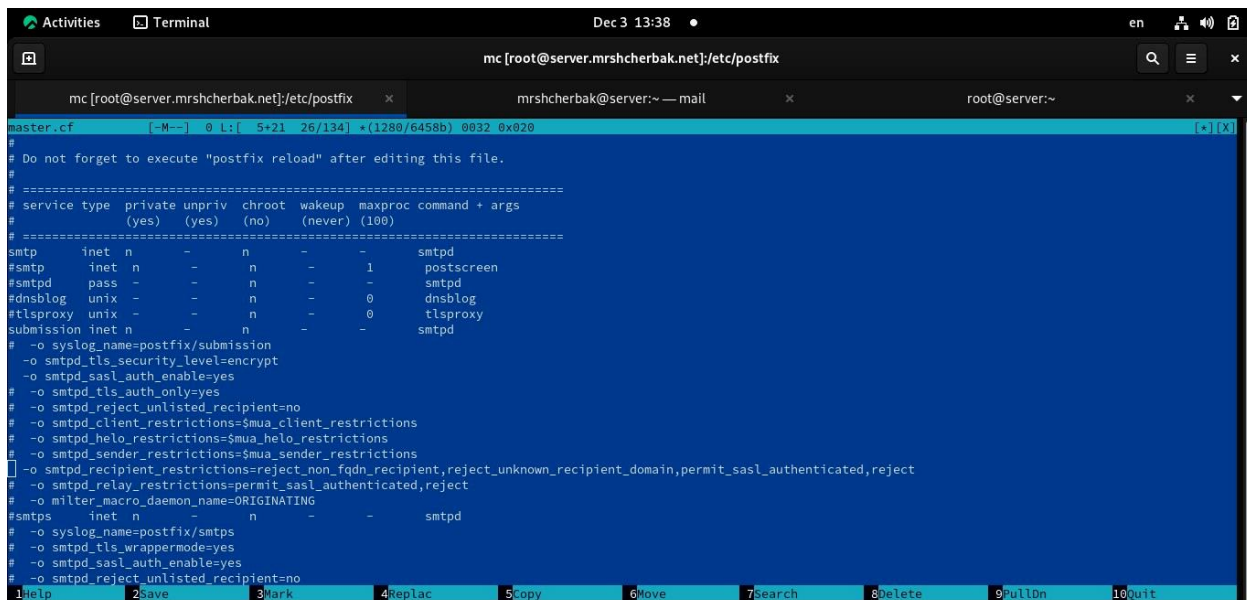


Рис.3.2. Редактирование файла /etc/postfix/master.cf

3. Настроила межсетевой экран, разрешив работать службе smtp-submission и перезапустила Postfix (рис.3.3).

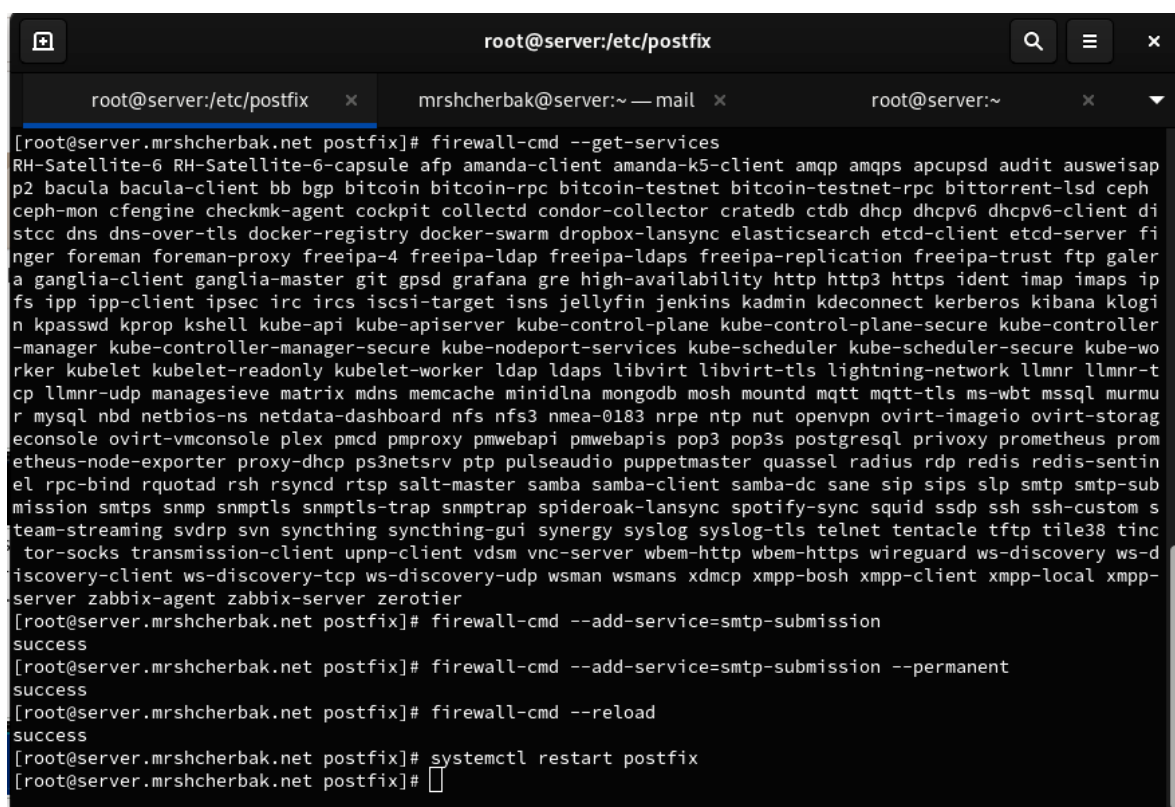


Рис.3.3. Выполнение команд

4. На клиенте подключилась к SMTP-серверу через 587-й порт посредством openssl и протестировала подключение по telnet, проверила аутентификацию (рис.3.4 – рис.3.6).

```
Activities Terminal Dec 3 14:15 en root@client:/etc/postfix

[root@client:mrshcherbak.net postfix]# openssl s_client -starttls smtp -crlf -connect server.mrshcherbak.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
 1:OU = IMAP server, CN = imap.example.com, emailAddress = postmaster@example.com
 a:PKEY: rsaEncryption, 3072 (01000101); sigalg: RSA-SHA256
 v:NotBefore: Dec  3 09:54:22 2023 GMT; NotAfter: Dec  2 09:54:22 2024 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIECjCCAggwwIBAgIUS1yNLAk9Ttvs8GnT9gFjYCAeT67QwDQVYKozZInvcNAQEL
BQAwMDEUMBIGA1UECwwLSU1BUICBZzX3Z2Z1xgTAI8BGNVBAWMEG1YXAUZXhhbXBs
ZS5jb20wJTAjBgkqhkiG9w0BCQEWBncvB3RtYXN0ZXJAZXhhbXBsZS5jb20wHhcN
MjMxMjAzMDk1NDIyMjc1MjMxMjMxMjMxMjMxMjMxMjMxMjMxMjMxMjMxMjMxMjMx
cnZlcjEEMBCGA1UEAwQwLmVudC5leFtGcG1LmNvYmVTElNCGCSG9S1b3DQEJARVY
cG9zZzG1nc3R1c3R1c3R1c3R1c3R1c3R1c3R1c3R1c3R1c3R1c3R1c3R1c3R1c3R1
AYoCggGBAKjXz4pU1Gve9aGes0e9XfKiYnjhlCDe1l1tYV9baARudgel8gotJMt
uR7J3heQD1VE8Rxs42/5Xdm3CqcxMU1SL0rPDWEYwa3K8KmlCapwJHPAxxojD
rGPOPaTh9txzE571cTT3Qfs02Praht5+xyz9CVA0aGp5lnPcbIAG6Esc6h4b9
CAZwmd3W+PS0dexNTuku1TBbpXEE8phfwSR45fughxzY4jUwhYVarBd9KGB2ARD
9P3v2+53o16Ej3Puyb7eR0gX0vrf0Z7eWzWuL5WCA8B9GkukVt3CeeoukLVpH
Bac5VLXvmayQ/cwFbnMBMbt5TzeBjPjFrH04YXfW0AHQ/SPyQ8teBNYpvmUZFFf4
2N3fVBnerMwSc0w1rrm0DtZ+9T7yp5xHSQ1zfg3reJnOV/cYR5RMrop2Rke3DgP
q9/QasGsUDHa7YM58ZKUGparjyu1+LNoDggTtT3VceBIXa103j1ZPwLXAKE9AXF
dBMak6prLwIDAQABozQWJARBglghkgBhvhCAQEEBAMCBKAwHQYDVROBBYEFN1q
qu+R8qRf4TqKwL5W1cldTFMA0GCSqGSI3DQEBwQAA41BgcCKwPw23DnpK2v
aQIctj50x2JtG6H8uShoK32yfr+oDbQuB64B7QSD6PGYU83ZkCQKf81ohvQEY78h
Xp8Nm4y37LAXLHrvDaMwp8Rc45dY4Ratj3LHg0B+6HwS61IivGAMfr2kvQuf08o9
HMAU2sL2q28+Y+72C26um1b30wVhe1uTEStV04DhrET7H1CxpDeZRZK7F8o1JY
5qSpLnLv1JorjH9nQgtwPclRWEtN14ckzpdazB2TXf0RHBUzzDatk8dV/e79Eq
1b2SVaHmzrVQhnt8j3dw0veCcgLkh0ryc2Dv25jzEEQ8Dkr10wplVwKRAWId
P8U+K8LcHIVK7v454qVnukKc4ZvbdQW817MK0antDqGu51XCvrtEBA4ypvNAFA0H
bst42Z7/rrrQKRCrAetNkpBjymscZFeySaIuRowe/aly1620z/uU/US4znmz3yLAO
KZ2nQqReYdGdGSFmk/+CbtzAvMbnK6Q5+CFJFoh0jx8RGaSU7Tc=
-----END CERTIFICATE-----
```

Рис.3.4. Подключение к SMTP-серверу через 587-й порт посредством openssl

```
Activities Terminal Dec 3 14:15 en root@client:/etc/postfix

subject=OU = IMAP server, CN = imap.example.com, emailAddress = postmaster@example.com
issuer=OU = IMAP server, CN = imap.example.com, emailAddress = postmaster@example.com
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2071 bytes and written 439 bytes
Verification error: self-signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 3072 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self-signed certificate)
---
250 CHUNKING
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
  Protocol : TLSv1.3
  Cipher : TLS_AES_256_GCM_SHA384
  Session-ID: FA2B395E5C3A73497519A7659C43FD3CF0F6E80CC7C00A216586672A6AFB281
  Session-ID-ctx:
  Resumption PSK: 171EF9ECBA73F12B28A457BD99F43FBC41ABBAE37DC7541B8448ED7BE0C72FE2E540A4D19F9584525533437CDEF1AF
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 7200 (seconds)
  TLS session ticket:
0000 - 02 97 0b 65 e7 ac 98 5d-e8 8d 07 46 be 76 4c 53 b...e...].F.vLS
0010 - 7c 96 05 17 e8 9d 21 f3-84 98 0e 97 6d 5d c8 88 [.....m]..
0020 - 4a 5e 48 e5 fb ef 23 c7-57 9f bb 82 aa 86 ab 2b J^H...#.W.....
0030 - 01 16 c7 b4 83 4f 44 5e-69 7c b8 06 5a ef 5c c2 ....00^1[.Z.\.
0040 - 64 7d 8f a9 41 3d 02 34-25 8b c7 e4 69 aa 6a c9 d).A-.4R...1.j.
0050 - 65 0a 96 ad 4e 27 53 fd-5e 23 15 e8 7c af 9c cd e....1S.#..|...
0060 - 29 73 70 77 e8 d2 c5 98-11 62 50 c0 7a 5e 69 07 )spw.....bP.z^..
```

Рис.3.5. Подключение к SMTP-серверу через 587-й порт посредством openssl

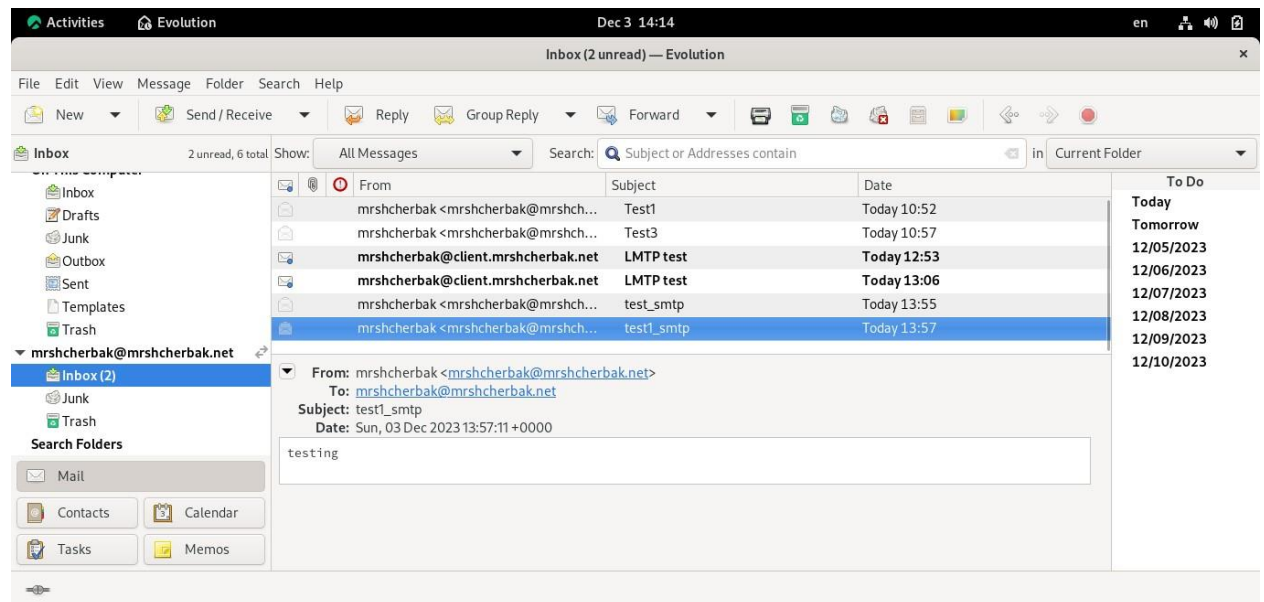


Рис.3.8. Проверка отправки почтовых сообщений с клиента

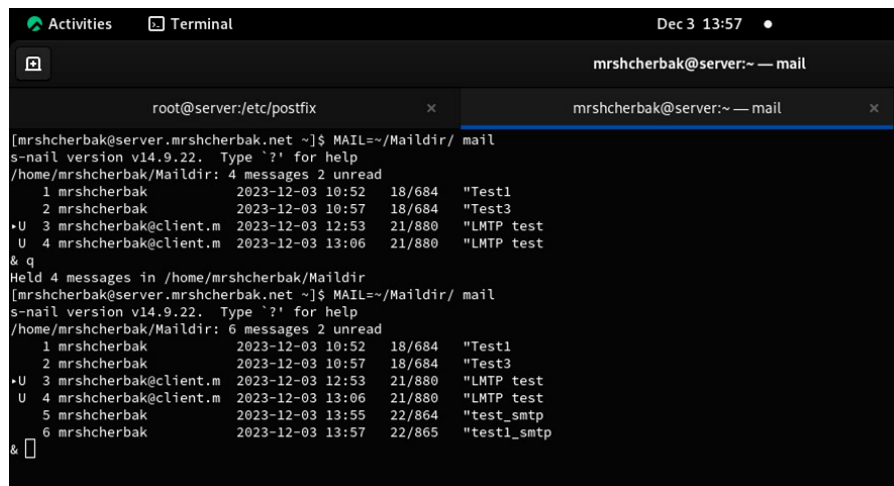


Рис.3.9. Проверка отправки почтовых сообщений с клиента

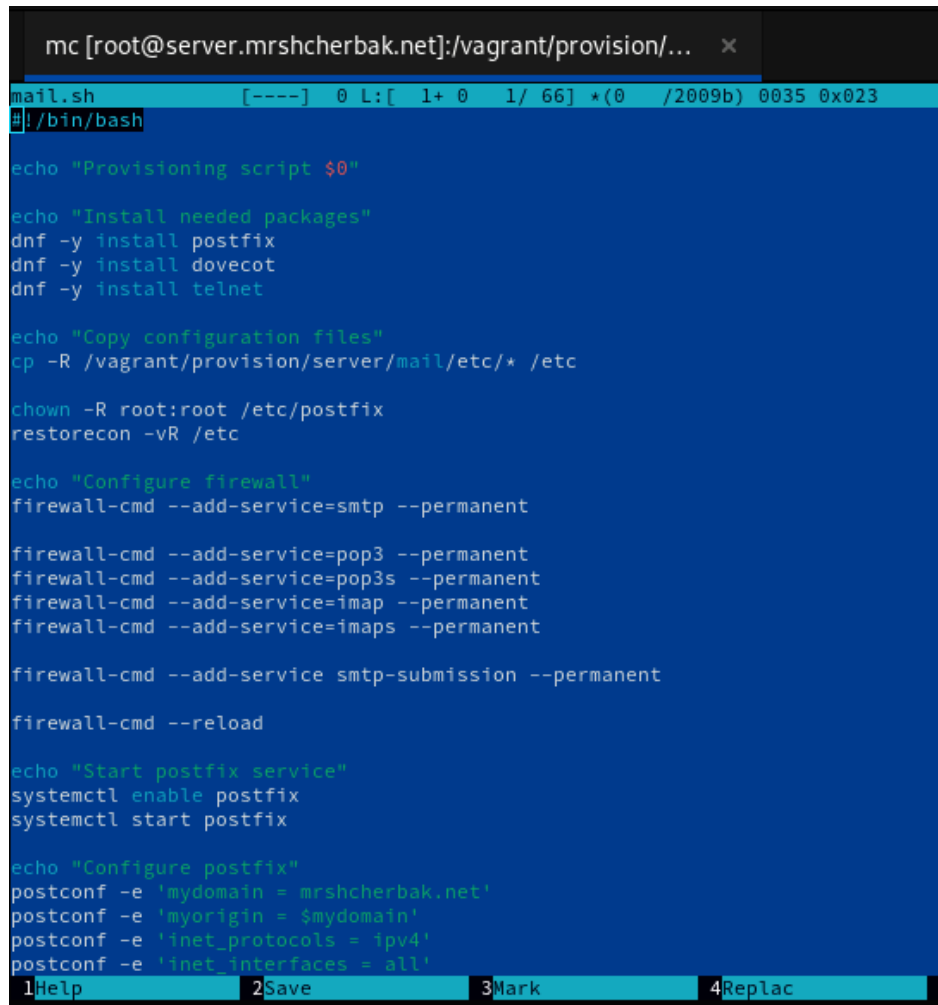
4. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`. В соответствующие подкаталоги поместила конфигурационные файлы Dovecot и Postfix (рис.4.1).

```
[root@server.mrshcherbak.net postfix]# cd /vagrant/provision/server
[root@server.mrshcherbak.net server]# cp -R /etc/dovecot/dovecot.conf /vagrant/provision/server/mail/etc/dovecot/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/dovecot.conf'? y
[root@server.mrshcherbak.net server]# cp -R /etc/dovecot/conf.d/10-master.conf /vagrant/provision/server/mail/etc/dovecot/conf.d/
[root@server.mrshcherbak.net server]# cp -R /etc/dovecot/conf.d/10-auth.conf /vagrant/provision/server/mail/etc/dovecot/conf.d/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/conf.d/10-auth.conf'? y
[root@server.mrshcherbak.net server]# cp -R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postfix/
[root@server.mrshcherbak.net server]#
```

Рис.4.1. Выполнение команд

2. Внесла соответствующие изменения по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh (рис.4.2 – рис.4.3).



```
mc [root@server.mrshcherbak.net]:/vagrant/provision/... x
mail.sh [----] 0 L: [ 1+ 0 1/ 66] *(0 /2009b) 0035 0x023
# /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

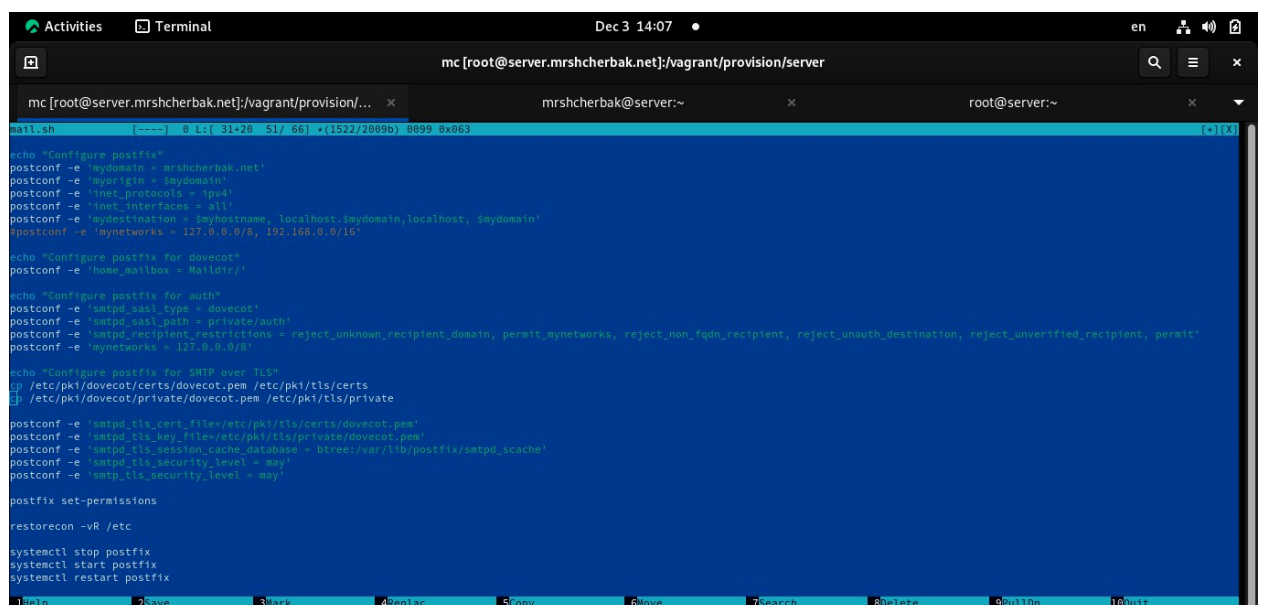
firewall-cmd --add-service smtp-submission --permanent

firewall-cmd --reload

echo "Start postfix service"
systemctl enable postfix
systemctl start postfix

echo "Configure postfix"
postconf -e 'mydomain = mrshcherbak.net'
postconf -e 'myorigin = $mydomain'
postconf -e 'inet_protocols = ipv4'
postconf -e 'inet_interfaces = all'
```

Рис.4.2. Содержимое файла /vagrant/provision/server/mail.sh



```
mc [root@server.mrshcherbak.net]:/vagrant/provision/server
mail.sh [----] 0 L: [ 31+20 51/ 66] *(1522/2009b) 0099 0x063
# /bin/bash

echo "Configure postfix"
postconf -e 'mydomain = mrshcherbak.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 = htree:/var/lib/postfix/smtpd_scache'
postconf -e 'smtpd_tls_security_level = may'
postconf -e 'smtpd_tls_security_level = may'

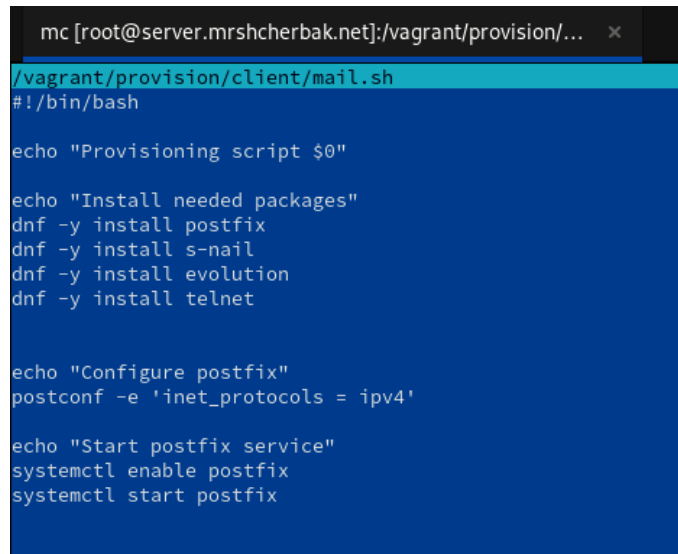
postfix set-permissions

restorecon -vR /etc

systemctl stop postfix
systemctl start postfix
systemctl restart postfix
```

Рис.4.3. Содержимое файла /vagrant/provision/server/mail.sh

3. Внесла изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet (рис.4.4).



```
mc [root@server.mrshcherbak.net]:vagrant/provision/... x
/vagrant/provision/client/mail.sh
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install postfix
dnf -y install s-nail
dnf -y install evolution
dnf -y install telnet

echo "Configure postfix"
postconf -e 'inet_protocols = ipv4'

echo "Start postfix service"
systemctl enable postfix
systemctl start postfix
```

Рис.4.4. Содержимое файла /vagrant/provision/client/mail.sh

Вывод: таким образом, в ходе выполнения л/р №10, я приобрела практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

Контрольные вопросы

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

Пример: auth_username_format = %Ln@%Ld

В данном примере %Ln представляет логин пользователя, а %Ld представляет домен.

2. Какие функции выполняет почтовый Relay-сервер?

Почтовый Relay-сервер выполняет функцию передачи почты между различными почтовыми серверами. Он принимает почту от клиента и передает ее по маршруту доставки к почтовому серверу назначения. Это позволяет почтовым серверам в сети взаимодействовать и передавать сообщения между различными доменами.

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

Угрозы безопасности при настройке почтового сервера как Relay-сервера могут включать в себя:

- возможность использования сервера злоумышленниками для пересылки спама или злоупотребления ресурсами.
- злоумышленники могут использовать Relay-сервер для создания высокой нагрузки на сервер, что может привести к отказу в обслуживании (DoS) или снижению производительности.
- злоумышленники могут попытаться перехватить почту, передаваемую через Relay-сервер, для получения конфиденциальной информации.
- злоумышленники могут использовать Relay-сервер для массовой отправки спама. Это может привести к блокировке вашего сервера почтовыми сервисами и плохой репутации вашего IP-адреса.
- Злоумышленники могут использовать ваш сервер для отправки вредоносных вложений. Это может включать в себя различные виды вредоносных программ, вредоносных ссылок и т. д.
- Злоумышленники могут попытаться использовать ваш почтовый сервер в качестве прокси-сервера для скрытия своего местоположения и исходного IP-адреса при проведении вредоносных действий.

Для предотвращения этих угроз, необходимо правильно настраивать Relay-сервер, включая ограничение доступа и введение механизмов аутентификации.