

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №10

дисциплина: Администрирование сетевых подсистем

Студент: Махорин Иван Сергеевич

Студ. билет № 1032211221

Группа: НПИбд-02-21

МОСКВА

2023 г.

Цель работы:

Целью данной работы является приобретение практических навыков по конфигурированию SMTP-сервера в части настройки аутентификации.

Выполнение работы:

На виртуальной машине server войдём под нашим пользователем и откроем терминал. Перейдём в режим суперпользователя (Рис. 1.1):

```
sudo -i
```

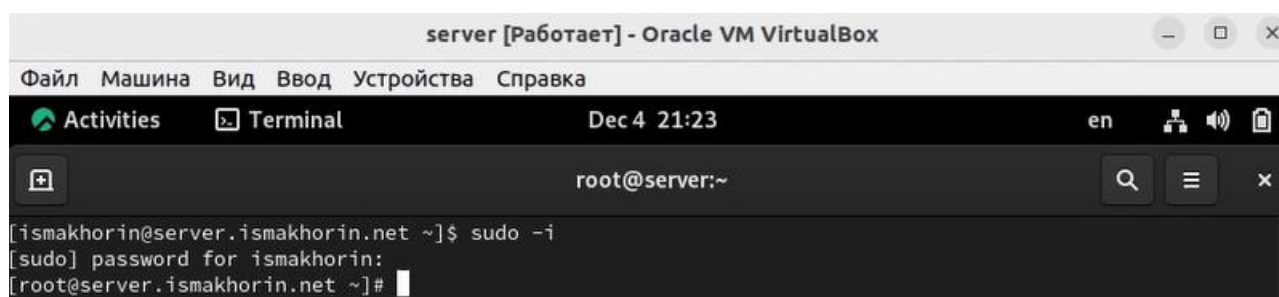
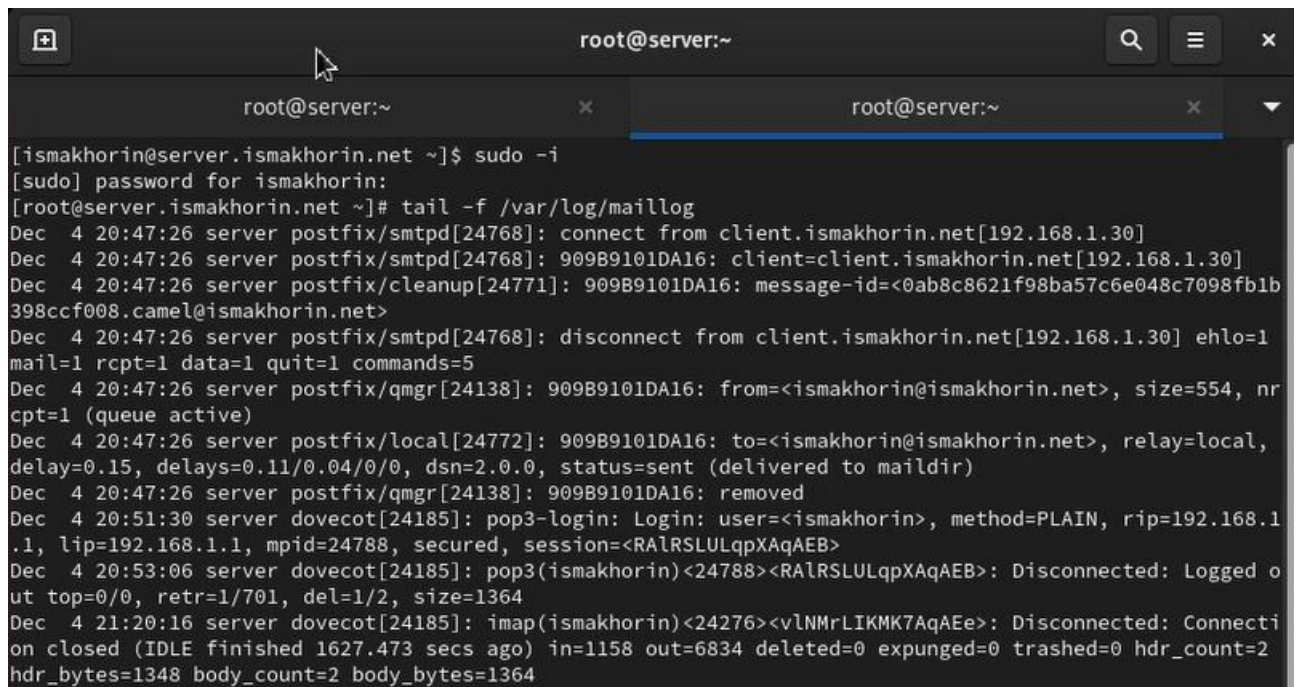


Рис. 1.1. Открытие режима суперпользователя на виртуальной машине server.

В дополнительном терминале запустим мониторинг работы почтовой службы (Рис. 1.2):

```
sudo -i
```

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

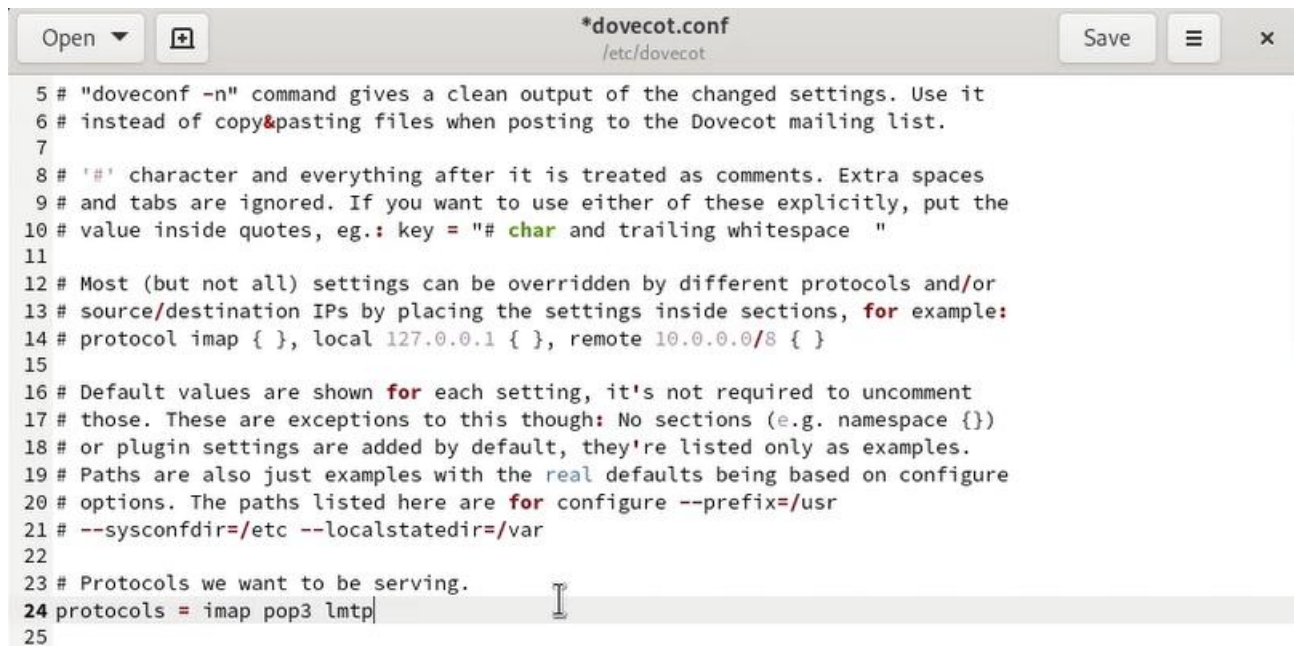


```
root@server:~  
[ismakhorin@server.ismakhorin.net ~]$ sudo -i  
[sudo] password for ismakhorin:  
[root@server.ismakhorin.net ~]# tail -f /var/log/maillog  
Dec  4 20:47:26 server postfix/smtpd[24768]: connect from client.ismakhorin.net[192.168.1.30]  
Dec  4 20:47:26 server postfix/smtpd[24768]: 909B9101DA16: client=client.ismakhorin.net[192.168.1.30]  
Dec  4 20:47:26 server postfix/cleanup[24771]: 909B9101DA16: message-id=<0ab8c8621f98ba57c6e048c7098fb1b398ccf008.camel@ismakhorin.net>  
Dec  4 20:47:26 server postfix/smtpd[24768]: disconnect from client.ismakhorin.net[192.168.1.30] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5  
Dec  4 20:47:26 server postfix/qmgr[24138]: 909B9101DA16: from=<ismakhorin@ismakhorin.net>, size=554, nr cpt=1 (queue active)  
Dec  4 20:47:26 server postfix/local[24772]: 909B9101DA16: to=<ismakhorin@ismakhorin.net>, relay=local, delay=0.15, delays=0.11/0.04/0/0, dsn=2.0.0, status=sent (delivered to maildir)  
Dec  4 20:47:26 server postfix/qmgr[24138]: 909B9101DA16: removed  
Dec  4 20:51:30 server dovecot[24185]: pop3-login: Login: user=<ismakhorin>, method=PLAIN, rip=192.168.1.1, lip=192.168.1.1, mpid=24788, secured, session=<RArSLULqpxAqAEB>  
Dec  4 20:53:06 server dovecot[24185]: pop3(ismakhorin)<24788><RArSLULqpxAqAEB>: Disconnected: Logged out top=0/0, retr=1/701, del=1/2, size=1364  
Dec  4 21:20:16 server dovecot[24185]: imap(ismakhorin)<24276><v\NMmrLIKMK7AqAEe>: Disconnected: Connection closed (IDLE finished 1627.473 secs ago) in=1158 out=6834 deleted=0 expunged=0 trashed=0 hdr_count=2 hdr_bytes=1348 body_count=2 body_bytes=1364
```

Рис. 1.2. Запуск в дополнительном терминале мониторинга работы почтовой службы.

Добавим в список протоколов, с которыми может работать Dovecot, протокол LMTP. Для этого в файле `/etc/dovecot/dovecot.conf` укажем (Рис. 1.3):

```
protocols = imap pop3 lmtp
```



```
5 # "doveconf -n" command gives a clean output of the changed settings. Use it
6 # instead of copy&pasting files when posting to the Dovecot mailing list.
7
8 # '#' character and everything after it is treated as comments. Extra spaces
9 # and tabs are ignored. If you want to use either of these explicitly, put the
10 # value inside quotes, eg.: key = "# char and trailing whitespace "
11
12 # Most (but not all) settings can be overridden by different protocols and/or
13 # source/destination IPs by placing the settings inside sections, for example:
14 # protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }
15
16 # Default values are shown for each setting, it's not required to uncomment
17 # those. These are exceptions to this though: No sections (e.g. namespace {})
18 # or plugin settings are added by default, they're listed only as examples.
19 # Paths are also just examples with the real defaults being based on configure
20 # options. The paths listed here are for configure --prefix=/usr
21 # --sysconfdir=/etc --localstatedir=/var
22
23 # Protocols we want to be serving.
24 protocols = imap pop3 lmtp
25
```

Рис. 1.3. Добавление в список протоколов, с которыми может работать Dovecot, протокола LMTP.

Настроим 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 из лабораторной работы (Рис. 1.4). 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.

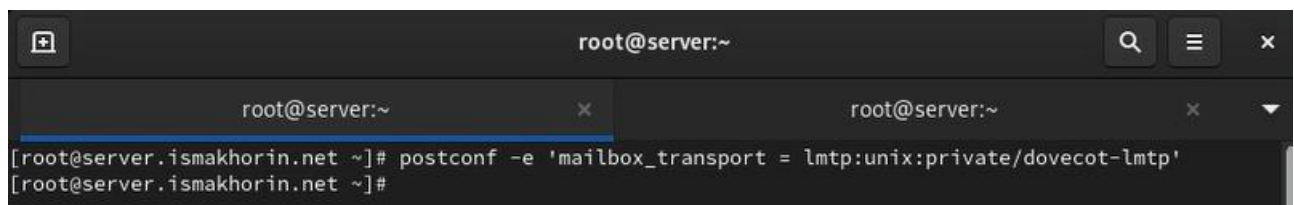


```
44 #ssl = yes
45 }
46 }
47
48 service submission-login {
49   inet_listener submission {
50     #port = 587
51   }
52 }
53
54 service lmtp {
55   unix_listener /var/spool/postfix/private/dovecot-lmtp {
56     group = postfix
57     user = postfix
58     mode = 0600
59   }
60 }
61 |
```

Рис. 1.4. Настройка в Dovecot сервиса lmtp для связи с Postfix.

Переопределим в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокеты (Рис. 1.5):

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



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

Рис. 1.5. Переопределение в Postfix с помощью postconf передачи сообщений не на прямую, а через заданный unix-сокеты.

В файле /etc/dovecot/conf.d/10-auth.conf зададим формат имени пользователя для аутентификации в форме логина пользователя без указания домена (Рис. 1.6):

```
auth_username_format = %Ln
```

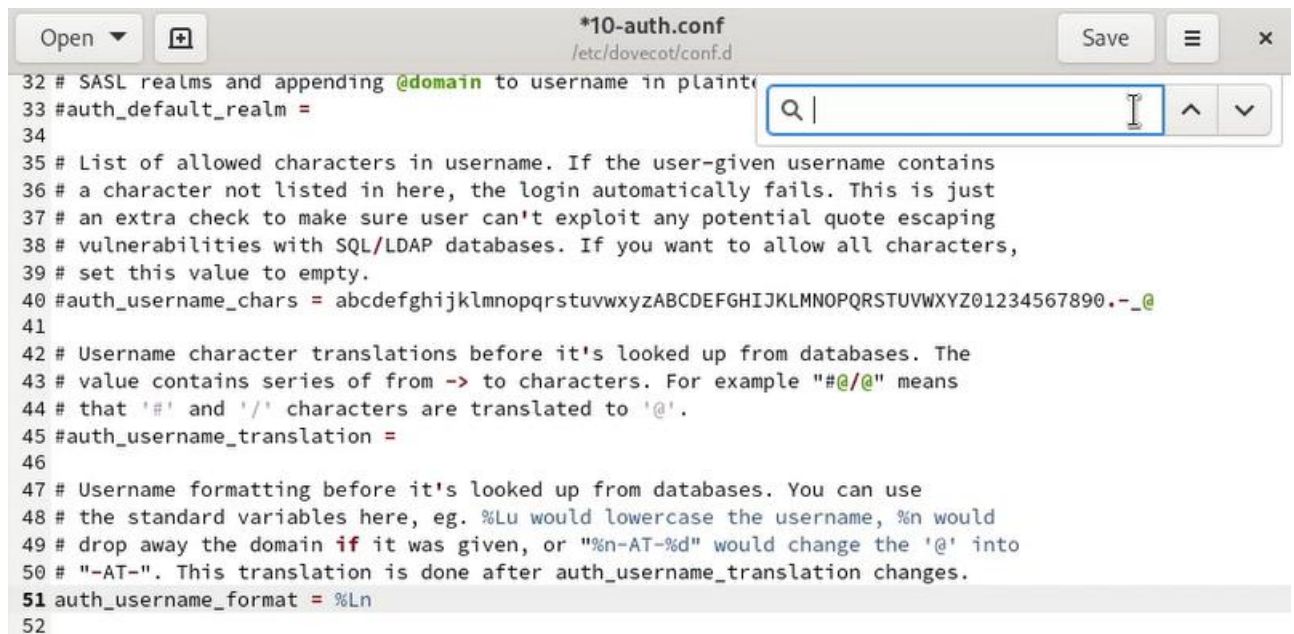


Рис. 1.6. Настройка в файле /etc/dovecot/conf.d/10-auth.conf формата имени пользователя для аутентификации в форме логина пользователя без указания домена.

Перезапустим Postfix и Dovecot (Рис. 1.7):

```
systemctl restart postfix
```

```
systemctl restart dovecot
```

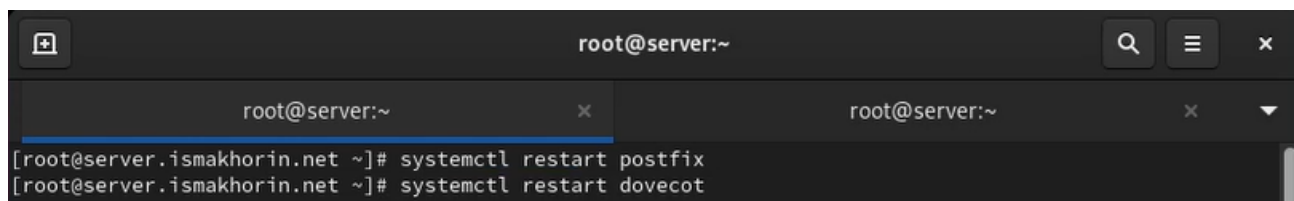


Рис. 1.7. Перезапуск Postfix и Dovecot.

Из-под учётной записи своего пользователя отправим письмо с клиента (Рис. 1.8):

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

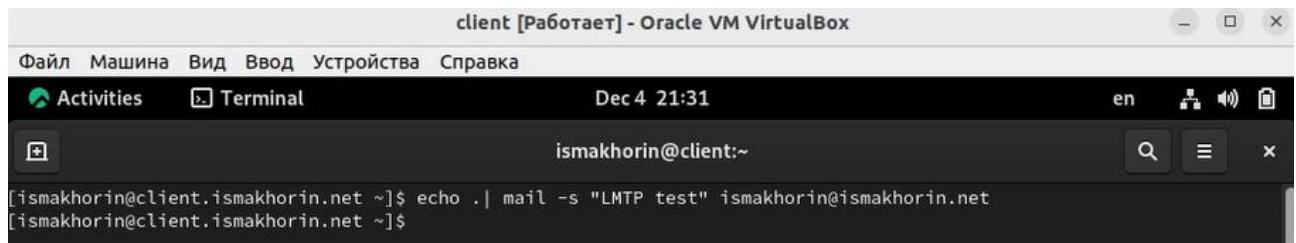



Рис. 1.8. Отправка из-под учётной записи своего пользователя письма с клиента.

После чего посмотрим содержание логов при мониторинге почтовой службы (Рис. 1.9):

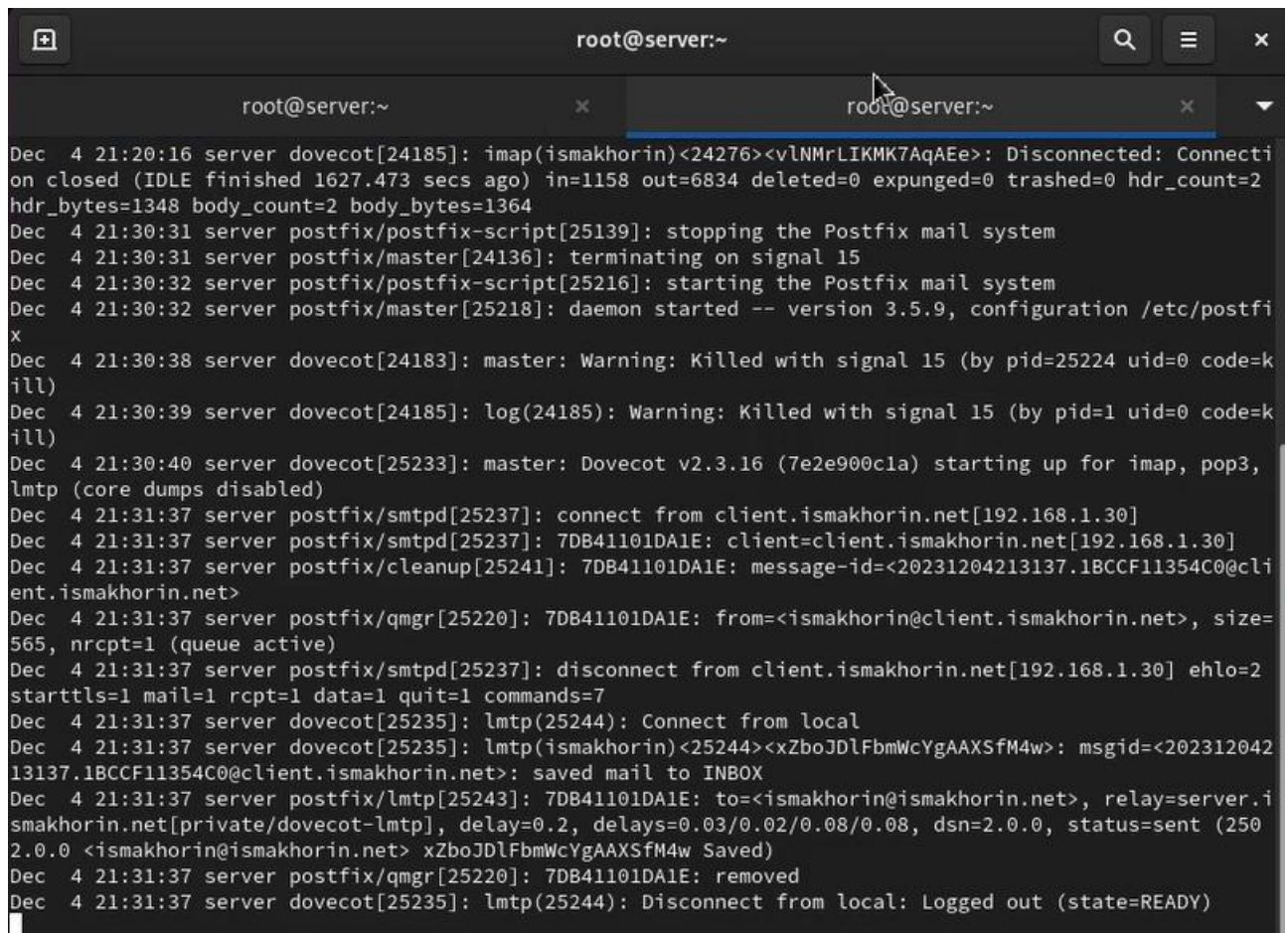
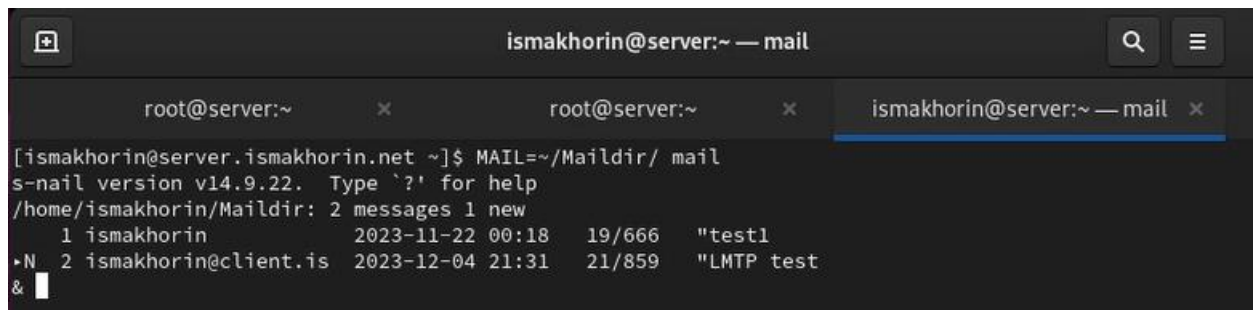


Рис. 1.9. Просмотр содержания логов при мониторинге почтовой службы.

На сервере посмотрим почтовый ящик пользователя (Рис. 1.10):

MAIL=~/.Maildir/ mail

A terminal window titled 'ismakhorin@server:~ — mail' showing the output of the 'MAIL' command. The output lists two messages in the mailbox: message 1 from 'ismakhorin' dated '2023-11-22 00:18' with subject 'test1', and message 2 from 'ismakhorin@client.is' dated '2023-12-04 21:31' with subject 'LMTP test'.

```
[ismakhorin@server.ismakhorin.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.22.  Type '?' for help
/home/ismakhorin/Maildir: 2 messages 1 new
 1 ismakhorin      2023-11-22 00:18    19/666    "test1
•N 2 ismakhorin@client.is 2023-12-04 21:31    21/859    "LMTP test
&
```

Рис. 1.10. Просмотр на сервере почтового ящика пользователя.

В файле `/etc/dovecot/conf.d/10-master.conf` определим службу аутентификации пользователей (Рис. 2.1):

A text editor window titled '*10-master.conf' showing the configuration for the 'auth' service in the file '/etc/dovecot/conf.d/10-master.conf'. The configuration defines two unix_listeners: one for 'auth' and one for 'auth-userdb'.

```
*10-master.conf
/etc/dovecot/conf.d

75
76 service submission {
77   # Max. number of SMTP Submission processes (connections)
78   #process_limit = 1024
79 }
80
81 service auth {
82   unix_listener /var/spool/postfix/private/auth {
83     group = postfix
84     user = postfix
85     mode = 0660
86   }
87   unix_listener auth-userdb {
88     mode = 0600
89     user = dovecot
90   }
91 }
92
```

Рис. 2.1. Определение в файле `/etc/dovecot/conf.d/10-master.conf` службы аутентификации пользователей.

Для Postfix зададим тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету:

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

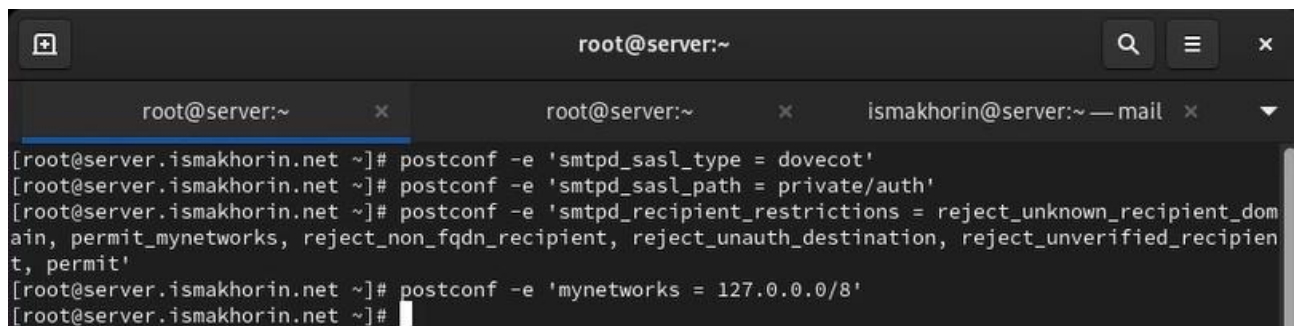
Далее настроим Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины (имеется в виду локальных пользователей

сервера), обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок (порядок указания опций имеет значение):

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

В настройках Postfix ограничим приём почты только локальным адресом SMTP-сервера сети (Рис. 2.2):

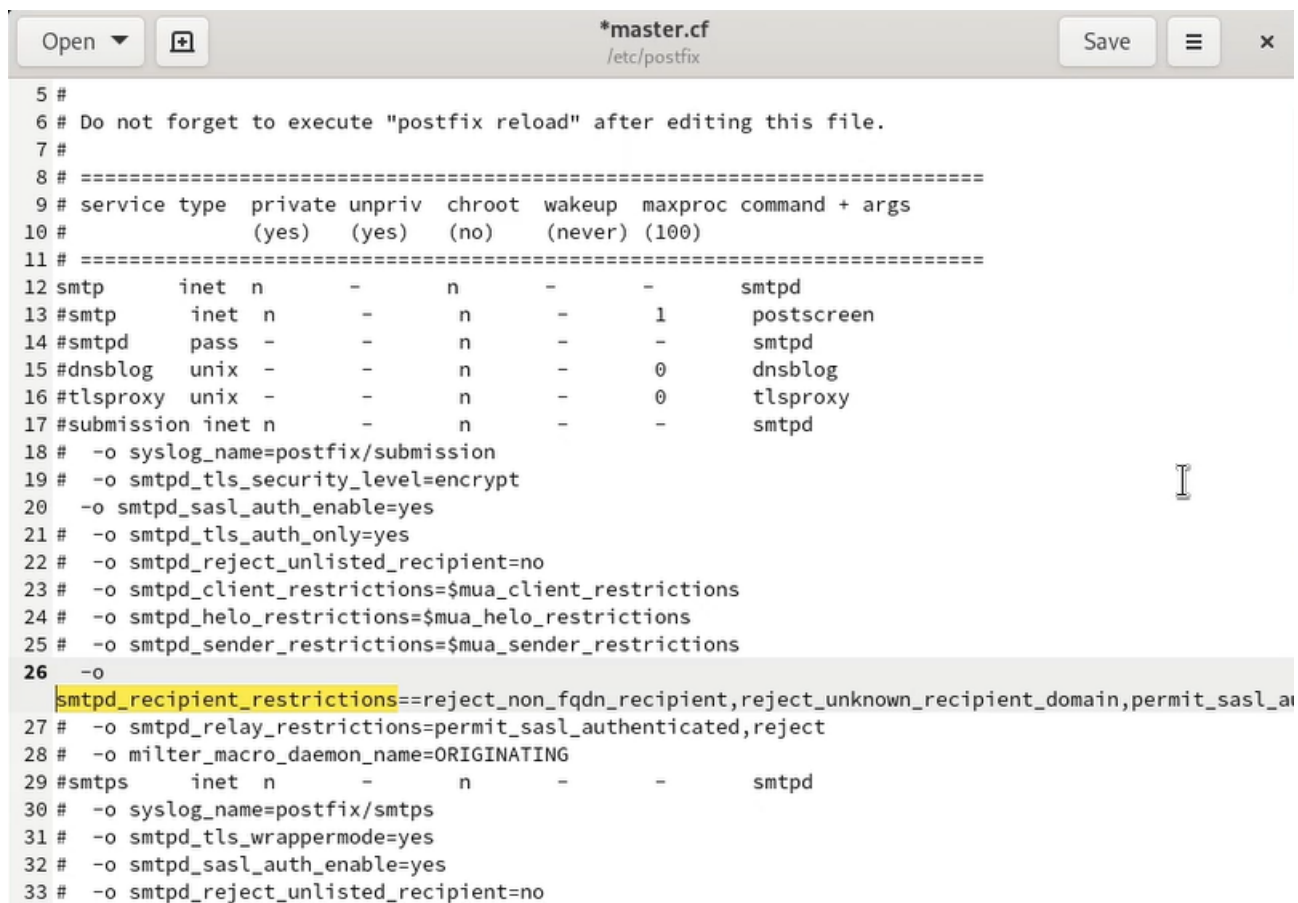
```
postconf -e 'mynetworks = 127.0.0.0/8'
```

A screenshot of a terminal window with a dark background. The window title is 'root@server:~'. There are three tabs: 'root@server:~', 'root@server:~', and 'ismakhorin@server:~ — mail'. The terminal shows the following commands and output:

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

Рис. 2.2. Настройка для Postfix типа аутентификации SASL для smtpd и пути к соответствующему unix-сокету, настройка Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины, ограничение в настройках Postfix приёма почты только локальным адресом SMTP-сервера сети.

Для проверки работы аутентификации временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Для этого в файле /etc/postfix/master.cf заменим строку (Рис. 2.3):



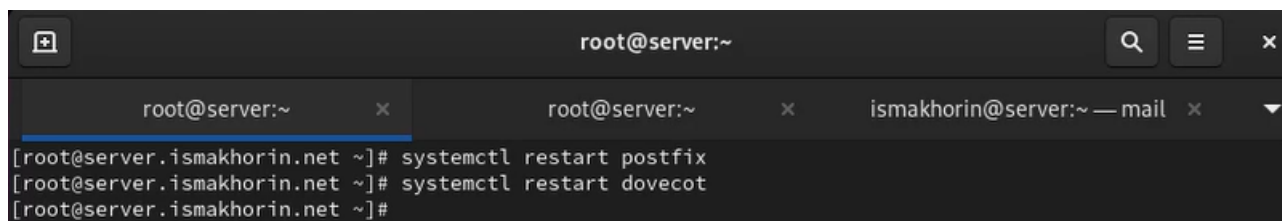
```
5 #
6 # Do not forget to execute "postfix reload" after editing this file.
7 #
8 # =====
9 # service type private unpriv chroot wakeup maxproc command + args
10 #          (yes)   (yes)   (no)    (never) (100)
11 # =====
12 smtp      inet  n       -       n       -       -       smtpd
13 #smtp     inet  n       -       n       -       1       postscreen
14 #smtpd    pass  -       -       n       -       -       smtpd
15 #dnsblog  unix  -       -       n       -       0       dnsblog
16 #tlsproxy unix  -       -       n       -       0       tlsproxy
17 #submission inet n       -       n       -       -       smtpd
18 # -o syslog_name=postfix/submission
19 # -o smtpd_tls_security_level=encrypt
20 # -o smtpd_sasl_auth_enable=yes
21 # -o smtpd_tls_auth_only=yes
22 # -o smtpd_reject_unlisted_recipient=no
23 # -o smtpd_client_restrictions=$mua_client_restrictions
24 # -o smtpd_helo_restrictions=$mua_helo_restrictions
25 # -o smtpd_sender_restrictions=$mua_sender_restrictions
26 # -o smtpd_recipient_restrictions=reject_non_fqdn_recipient, reject_unknown_recipient_domain, permit_sasl_authenticated, reject
27 # -o smtpd_relay_restrictions=permit_sasl_authenticated, reject
28 # -o milter_macro_daemon_name=ORIGINATING
29 #smtps    inet  n       -       n       -       -       smtpd
30 # -o syslog_name=postfix/smtps
31 # -o smtpd_tls_wrappermode=yes
32 # -o smtpd_sasl_auth_enable=yes
33 # -o smtpd_reject_unlisted_recipient=no
```

Рис. 2.3. Временный запуск для проверки работы аутентификации SMTP-сервера (порт 25) с возможностью аутентификации.

Затем перезапустим Postfix и Dovecot (Рис. 2.4):

```
systemctl restart postfix
```

```
systemctl restart dovecot
```



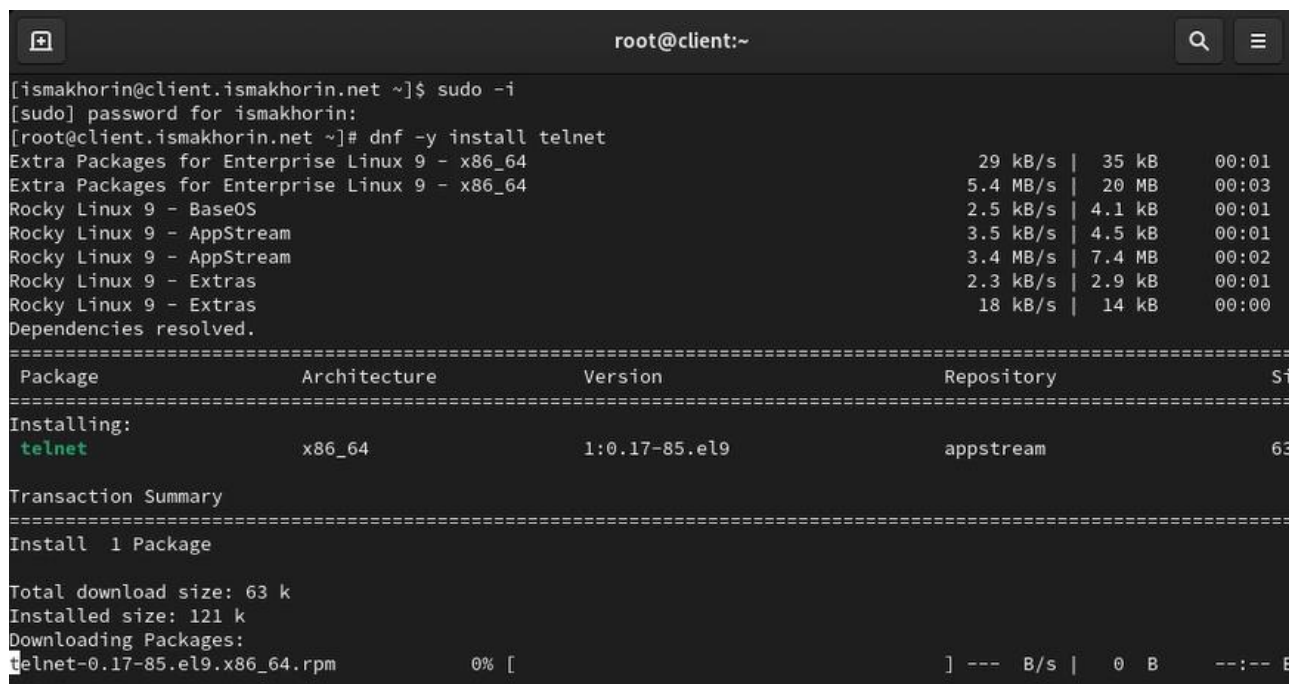
```
root@server:~
[root@server.ismakhorin.net ~]# systemctl restart postfix
[root@server.ismakhorin.net ~]# systemctl restart dovecot
[root@server.ismakhorin.net ~]#
```

Рис. 2.4. Перезапуск Postfix и Dovecot.

На клиенте установим telnet (Рис. 2.5):

```
sudo -i
```

```
dnf -y install telnet
```



```
root@client:~  
[ismakhorin@client.ismakhorin.net ~]$ sudo -i  
[sudo] password for ismakhorin:  
[root@client.ismakhorin.net ~]# dnf -y install telnet  
Extra Packages for Enterprise Linux 9 - x86_64          29 kB/s | 35 kB      00:01  
Extra Packages for Enterprise Linux 9 - x86_64          5.4 MB/s | 20 MB     00:03  
Rocky Linux 9 - BaseOS                                  2.5 kB/s | 4.1 kB     00:01  
Rocky Linux 9 - AppStream                               3.5 kB/s | 4.5 kB     00:01  
Rocky Linux 9 - AppStream                               3.4 MB/s | 7.4 MB     00:02  
Rocky Linux 9 - Extras                                  2.3 kB/s | 2.9 kB     00:01  
Rocky Linux 9 - Extras                                  18 kB/s | 14 kB      00:00  
Dependencies resolved.  
=====
```

Package	Architecture	Version	Repository	Size
telnet	x86_64	1:0.17-85.el9	appstream	63

```
=====
```

Transaction Summary

=====

Install 1 Package

Total download size: 63 k
Installed size: 121 k
Downloading Packages:
telnet-0.17-85.el9.x86_64.rpm 0% [] --- B/s | 0 B --:-- E

Рис. 2.5. Установка на клиенте telnet.

На клиенте получим строку для аутентификации:

```
printf 'ismakhorin\x00username\x00123456' | base64
```

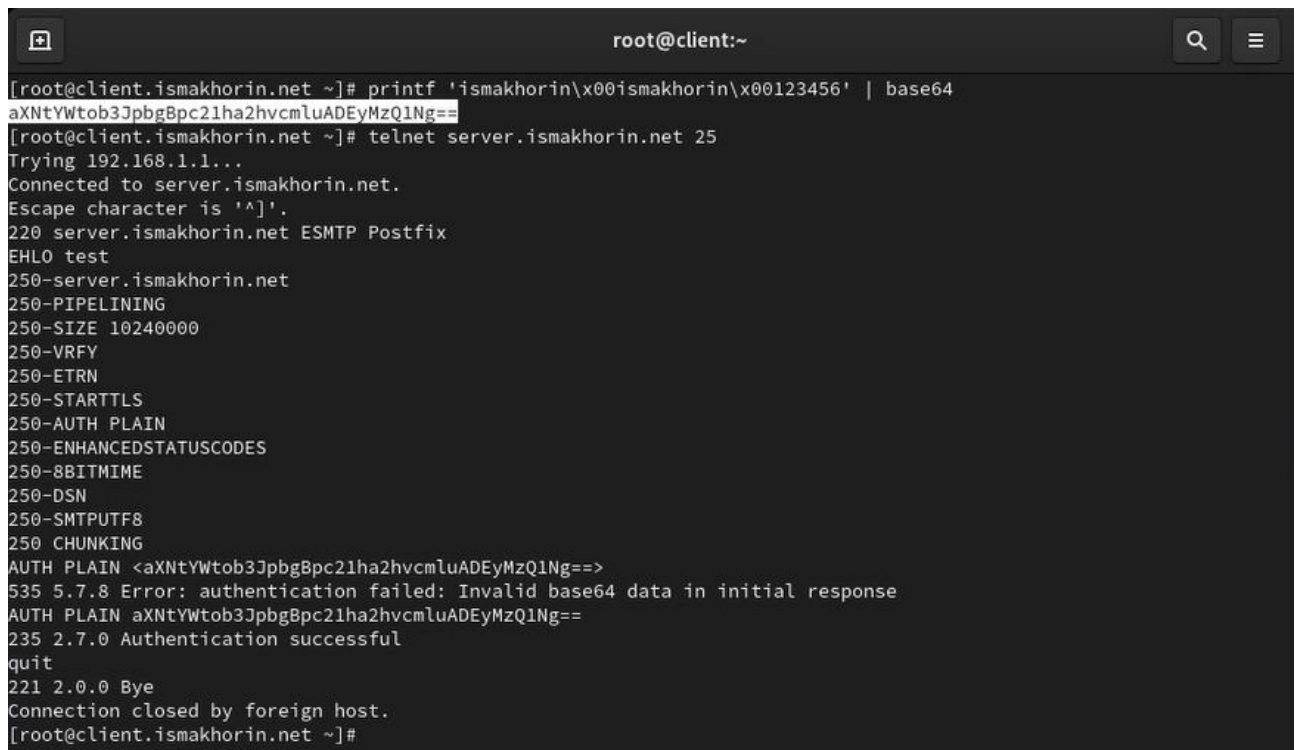
В качестве результата получим строку для аутентификации в формате base64. После чего подключимся на клиенте к SMTP-серверу посредством telnet:

```
telnet server.ismakhorin.net 25
```

Теперь протестируем соединение, введя EHLO test и проверим авторизацию, задав:

```
AUTH PLAIN <СДА>
```

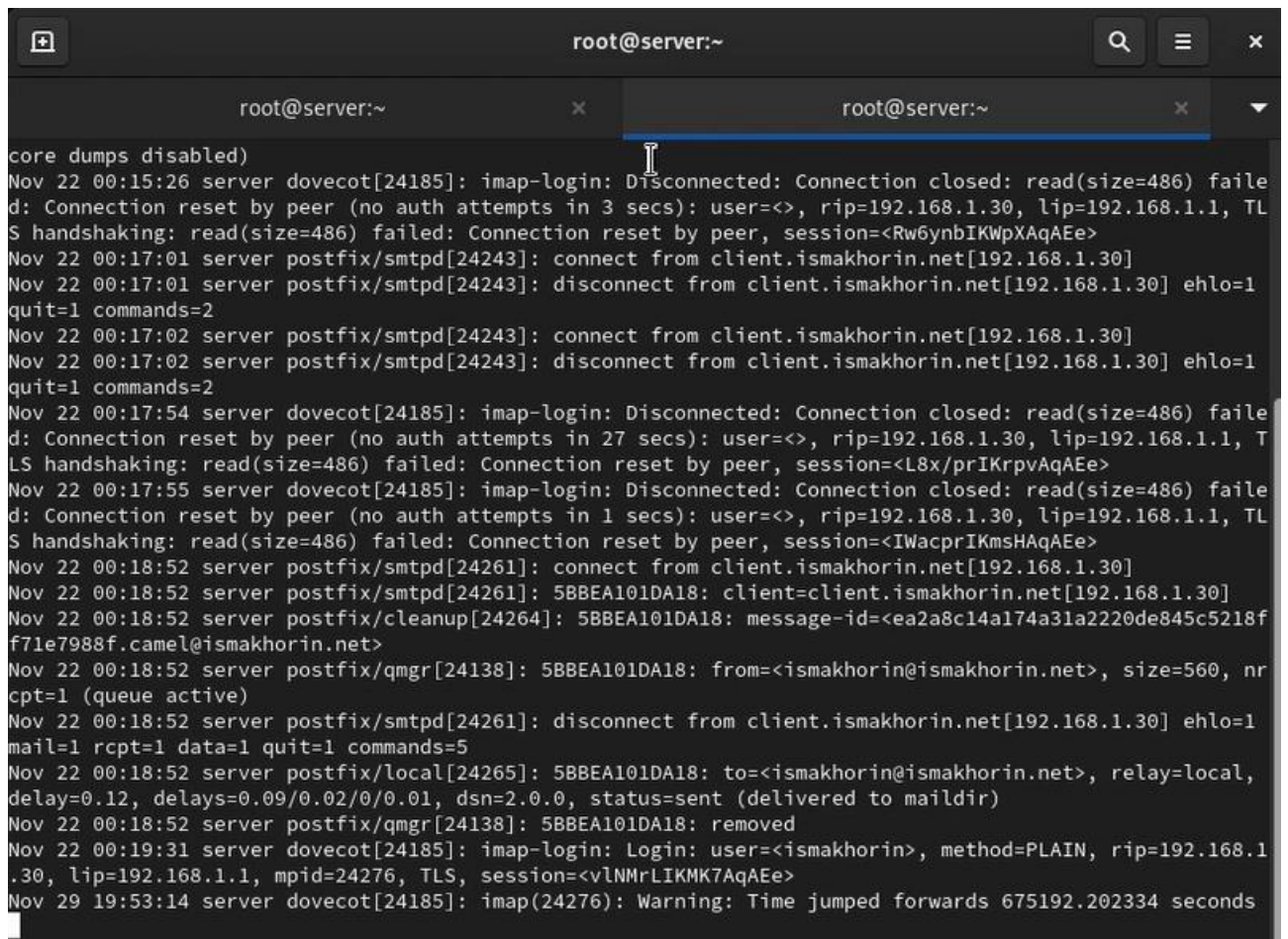
Завершим сессию telnet на клиенте (Рис. 2.6):

A terminal window titled 'root@client:~' showing a telnet session with an SMTP server. The user first generates a base64 encoded string using 'printf' and then uses 'telnet' to connect to 'server.ismakhorin.net' on port 25. The session shows standard SMTP greetings, a successful PLAIN authentication, and a final 'quit' command. The terminal output is as follows:

```
[root@client.ismakhorin.net ~]# printf 'ismakhorin\x00ismakhorin\x00123456' | base64
aXNtYWtob3JpbG8pc21ha2hvcmluADEyMzQ1Ng==
[root@client.ismakhorin.net ~]# telnet server.ismakhorin.net 25
Trying 192.168.1.1...
Connected to server.ismakhorin.net.
Escape character is '^]'.
220 server.ismakhorin.net ESMTP Postfix
EHLO test
250-server.ismakhorin.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 <aXNtYWtob3JpbG8pc21ha2hvcmluADEyMzQ1Ng==>
535 5.7.8 Error: authentication failed: Invalid base64 data in initial response
AUTH PLAIN aXNtYWtob3JpbG8pc21ha2hvcmluADEyMzQ1Ng==
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
Connection closed by foreign host.
[root@client.ismakhorin.net ~]#
```

Рис. 2.6. Получение на клиенте строки для аутентификации, подключение на клиенте к SMTP-серверу посредством telnet, тестирование соединения, проверка авторизации и завершение сессии telnet на клиенте.

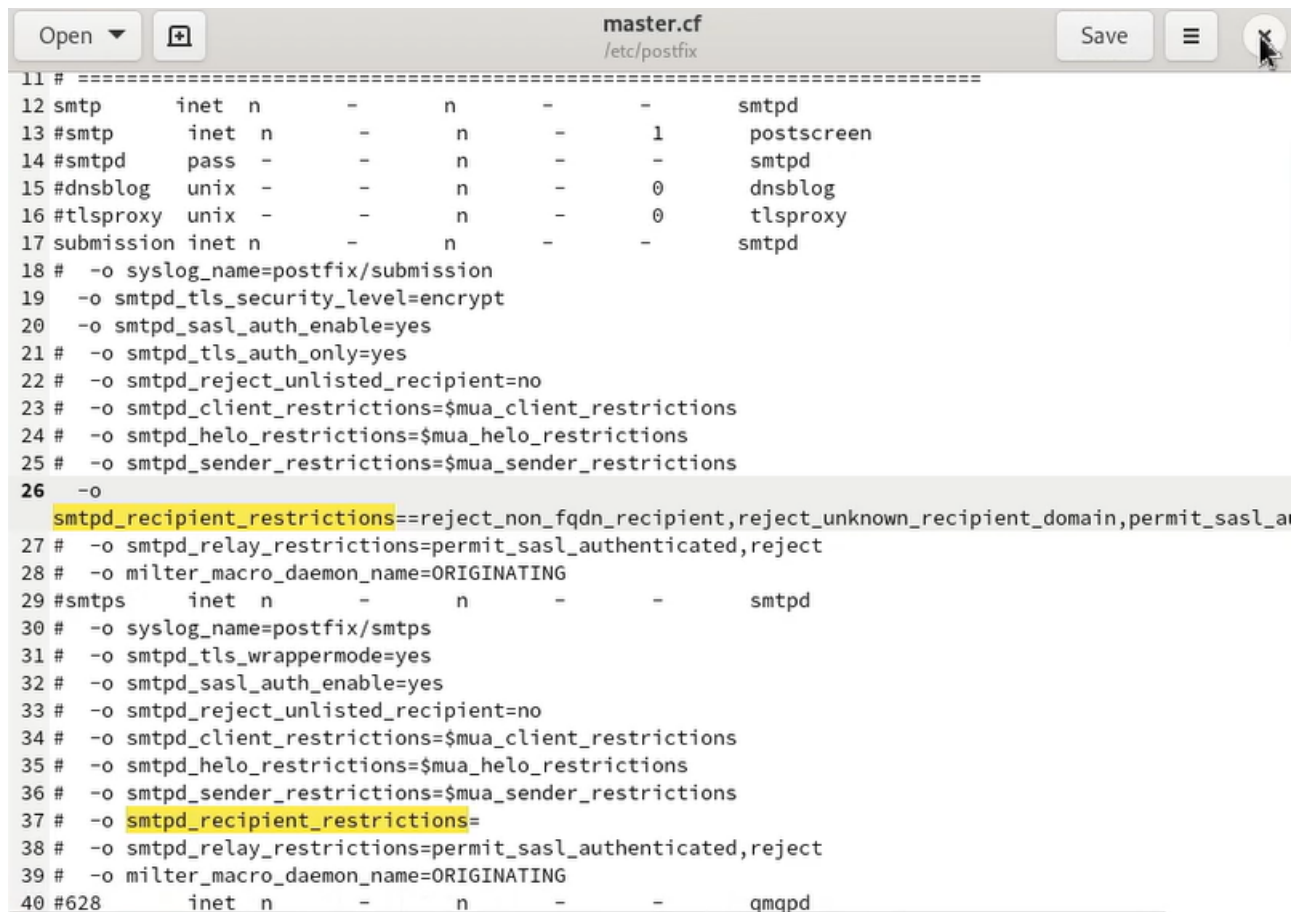
Настроим на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно скопируем необходимые файлы сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги (чтобы не было проблем с SELinux). Далее сконфигурируем Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности (Рис. 3.1):



```
core dumps disabled)
Nov 22 00:15:26 server dovecot[24185]: imap-login: Disconnected: Connection closed: read(size=486) failed: Connection reset by peer (no auth attempts in 3 secs): user=<>, rip=192.168.1.30, lip=192.168.1.1, TLS handshaking: read(size=486) failed: Connection reset by peer, session=<Rw6ynbIKWpXAqAEe>
Nov 22 00:17:01 server postfix/smtpd[24243]: connect from client.ismakhorin.net[192.168.1.30]
Nov 22 00:17:01 server postfix/smtpd[24243]: disconnect from client.ismakhorin.net[192.168.1.30] ehlo=1 quit=1 commands=2
Nov 22 00:17:02 server postfix/smtpd[24243]: connect from client.ismakhorin.net[192.168.1.30]
Nov 22 00:17:02 server postfix/smtpd[24243]: disconnect from client.ismakhorin.net[192.168.1.30] ehlo=1 quit=1 commands=2
Nov 22 00:17:54 server dovecot[24185]: imap-login: Disconnected: Connection closed: read(size=486) failed: Connection reset by peer (no auth attempts in 27 secs): user=<>, rip=192.168.1.30, lip=192.168.1.1, TLS handshaking: read(size=486) failed: Connection reset by peer, session=<L8x/prIKrpvAqAEe>
Nov 22 00:17:55 server dovecot[24185]: imap-login: Disconnected: Connection closed: read(size=486) failed: Connection reset by peer (no auth attempts in 1 secs): user=<>, rip=192.168.1.30, lip=192.168.1.1, TLS handshaking: read(size=486) failed: Connection reset by peer, session=<IWacprIKmsHAqAEe>
Nov 22 00:18:52 server postfix/smtpd[24261]: connect from client.ismakhorin.net[192.168.1.30]
Nov 22 00:18:52 server postfix/smtpd[24261]: 5BBEA101DA18: client=client.ismakhorin.net[192.168.1.30]
Nov 22 00:18:52 server postfix/cleanup[24264]: 5BBEA101DA18: message-id=<ea2a8c14a174a31a2220de845c5218ff71e7988f.camel@ismakhorin.net>
Nov 22 00:18:52 server postfix/qmgr[24138]: 5BBEA101DA18: from=<ismakhorin@ismakhorin.net>, size=560, nr_cpt=1 (queue active)
Nov 22 00:18:52 server postfix/smtpd[24261]: disconnect from client.ismakhorin.net[192.168.1.30] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Nov 22 00:18:52 server postfix/local[24265]: 5BBEA101DA18: to=<ismakhorin@ismakhorin.net>, relay=local, delay=0.12, delays=0.09/0.02/0/0.01, dsn=2.0.0, status=sent (delivered to maildir)
Nov 22 00:18:52 server postfix/qmgr[24138]: 5BBEA101DA18: removed
Nov 22 00:19:31 server dovecot[24185]: imap-login: Login: user=<ismakhorin>, method=PLAIN, rip=192.168.1.30, lip=192.168.1.1, mpid=24276, TLS, session=<vLNMrLIKMK7AqAEe>
Nov 29 19:53:14 server dovecot[24185]: imap(24276): Warning: Time jumped forwards 675192.202334 seconds
```

Рис. 3.1. Настройка на сервере TLS и предварительное копирование необходимых файлов сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги. Настройка конфигурации Postfix.

Для того чтобы запустить SMTP-сервер на 587-м порту, в файле /etc/postfix/master.cf заменим строки (рис. 3.2):



```
11 # =====
12 smtp      inet  n      -      n      -      -      smtpd
13 #smtp      inet  n      -      n      -      1      postscreen
14 #smtpd     pass  -      -      n      -      -      smtpd
15 #dnsblog   unix  -      -      n      -      0      dnsblog
16 #tlsproxy  unix  -      -      n      -      0      tlsproxy
17 submission inet  n      -      n      -      -      smtpd
18 # -o syslog_name=postfix/submission
19 # -o smtpd_tls_security_level=encrypt
20 # -o smtpd_sasl_auth_enable=yes
21 # -o smtpd_tls_auth_only=yes
22 # -o smtpd_reject_unlisted_recipient=no
23 # -o smtpd_client_restrictions=$mua_client_restrictions
24 # -o smtpd_helo_restrictions=$mua_helo_restrictions
25 # -o smtpd_sender_restrictions=$mua_sender_restrictions
26 # -o smtpd_recipient_restrictions=reject_non_fqdn_recipient, reject_unknown_recipient_domain, permit_sasl_authenticated, reject
27 # -o smtpd_relay_restrictions=permit_sasl_authenticated, reject
28 # -o milter_macro_daemon_name=ORIGINATING
29 #smtps     inet  n      -      n      -      -      smtpd
30 # -o syslog_name=postfix/smtps
31 # -o smtpd_tls_wrappermode=yes
32 # -o smtpd_sasl_auth_enable=yes
33 # -o smtpd_reject_unlisted_recipient=no
34 # -o smtpd_client_restrictions=$mua_client_restrictions
35 # -o smtpd_helo_restrictions=$mua_helo_restrictions
36 # -o smtpd_sender_restrictions=$mua_sender_restrictions
37 # -o smtpd_recipient_restrictions=
38 # -o smtpd_relay_restrictions=permit_sasl_authenticated, reject
39 # -o milter_macro_daemon_name=ORIGINATING
40 #628       inet  n      -      n      -      -      qmqpd
```

Рис. 3.2. Замена строк в файле /etc/postfix/master.cf для того чтобы запустить SMTP-сервер на 587-м порту.

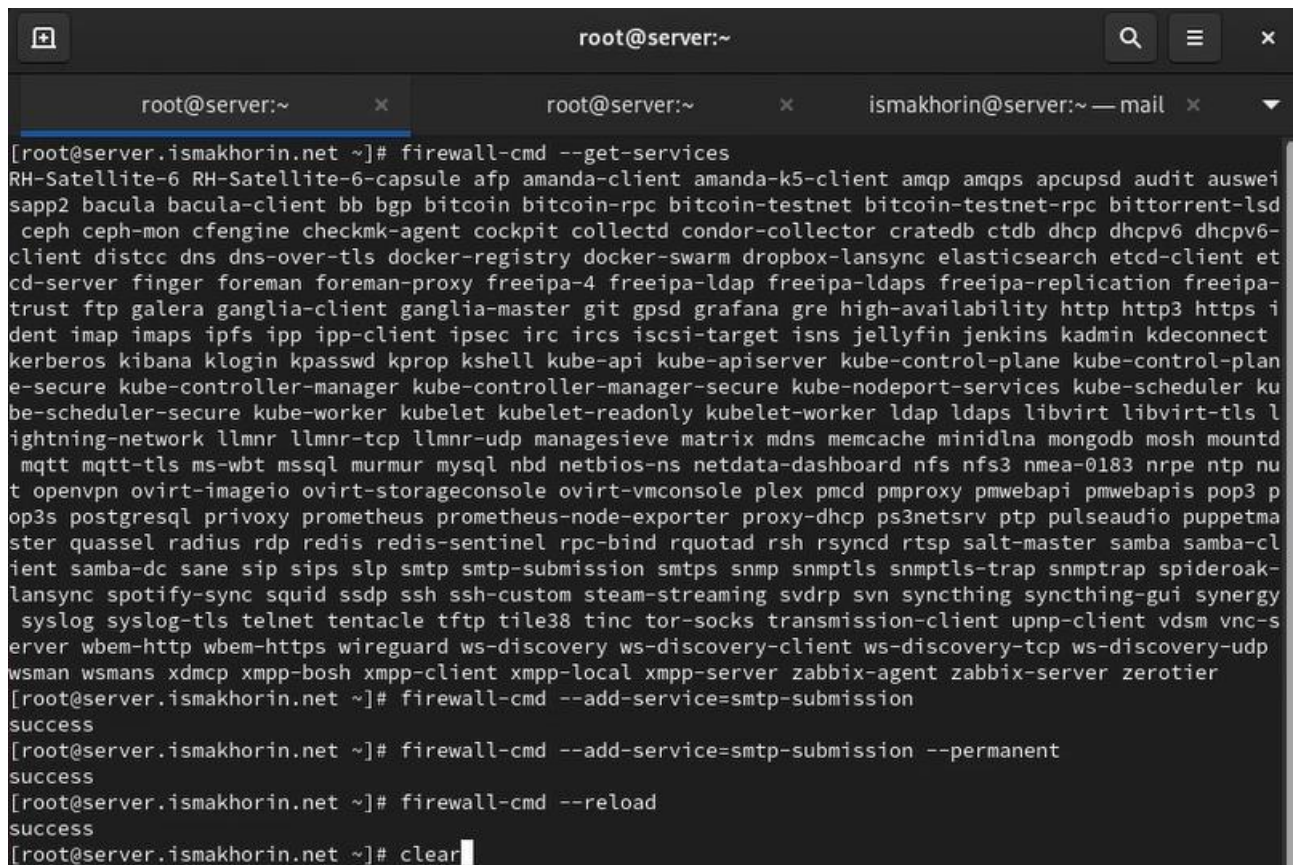
Настроим межсетевой экран, разрешив работать службе smtp-submission (рис. 3.3):

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

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

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

```
firewall-cmd --reload
```

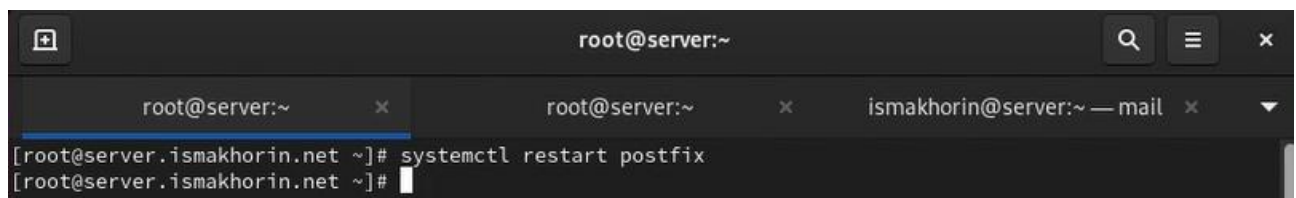



```
root@server:~  
[root@server.ismakhorin.net ~]# firewall-cmd --get-services  
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit auswei  
sapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd  
ceph ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcpv6-  
client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client et  
cd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-  
trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https i  
dent imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdeconnect  
kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plan  
e-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler ku  
be-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls l  
ightning-network llmnr llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd  
mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nu  
t openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 p  
op3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulseaudio puppetma  
ster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-cl  
ient samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-  
lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy  
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsd vnc-s  
erver wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp  
wsman wsmans xdmpc xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier  
[root@server.ismakhorin.net ~]# firewall-cmd --add-service=smtp-submission  
success  
[root@server.ismakhorin.net ~]# firewall-cmd --add-service=smtp-submission --permanent  
success  
[root@server.ismakhorin.net ~]# firewall-cmd --reload  
success  
[root@server.ismakhorin.net ~]# clear
```

Рис. 3.3. Настройка межсетевого экрана, разрешив работать службе smtp-submission.

Перезапустим Postfix (рис. 3.4):

systemctl restart postfix



```
root@server:~  
[root@server.ismakhorin.net ~]# systemctl restart postfix  
[root@server.ismakhorin.net ~]#
```

Рис. 3.4. Перезапуск Postfix.

На клиенте подключимся к SMTP-серверу через 587-й порт посредством openssl и протестируем подключение по telnet, проверим аутентификацию (рис. 3.5):

```
root@client:~  
0050 - 23 96 58 58 2e e4 5c 4a-81 61 d8 45 85 d0 e6 60 #.XX..\J.a.E...`  
0060 - f2 40 95 01 d0 f8 f7 7e-c5 2b b7 38 3f b1 49 d0 .@.....~+.8?.I.  
0070 - eb d2 d4 03 63 09 23 9a-bd b1 a1 76 b6 dd 52 54 ....c.#....v..RT  
0080 - f6 0c f4 af 2d 40 8a a8-33 ac 87 c3 51 ec 16 6b ....-@..3...Q..k  
0090 - e2 23 f3 f5 fd c7 b5 76-c4 bf 7d 5c 96 58 8e 5f .#.....v..}\X._  
00a0 - f0 e2 b1 07 a4 74 d5 bc-ab 3e 39 dd 3d cb a0 da .....t...>9.=...  
00b0 - 82 77 6e a9 42 65 3f 5c-f4 de bd c3 77 8f 94 ac .wn.Be?\....w...  
00c0 - 94 bf 37 b5 59 ff 12 e7-f6 02 07 16 5d 14 53 34 ..7.Y.....].S4  
  
Start Time: 1701727007  
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.ismakhorin.net  
250-PIPELINING  
250-SIZE 10240000  
250-VRFY  
250-ETRN  
250-AUTH PLAIN  
250-ENHANCEDSTATUSCODES  
250-8BITMIME  
250-DSN  
250-SMTPUTF8  
250 CHUNKING  
AUTH PLAIN aXNtYWtob3JpbG9pc21ha2hvcmluADEyMzQ1Ng==  
235 2.7.0 Authentication successful  
quit  
221 2.0.0 Bye  
closed  
[root@client.ismakhorin.net ~]#
```

Рис. 3.5. Подключение на клиенте к SMTP-серверу через 587-й порт посредством openssl, тестирование подключения по telnet и проверка аутентификации.

Проверим корректность отправки почтовых сообщений с клиента посредством почтового клиента Evolution, предварительно скорректировав настройки учётной записи, а именно для SMTP-сервера укажем порт 587, STARTTLS и обычный пароль (рис. 3.6):

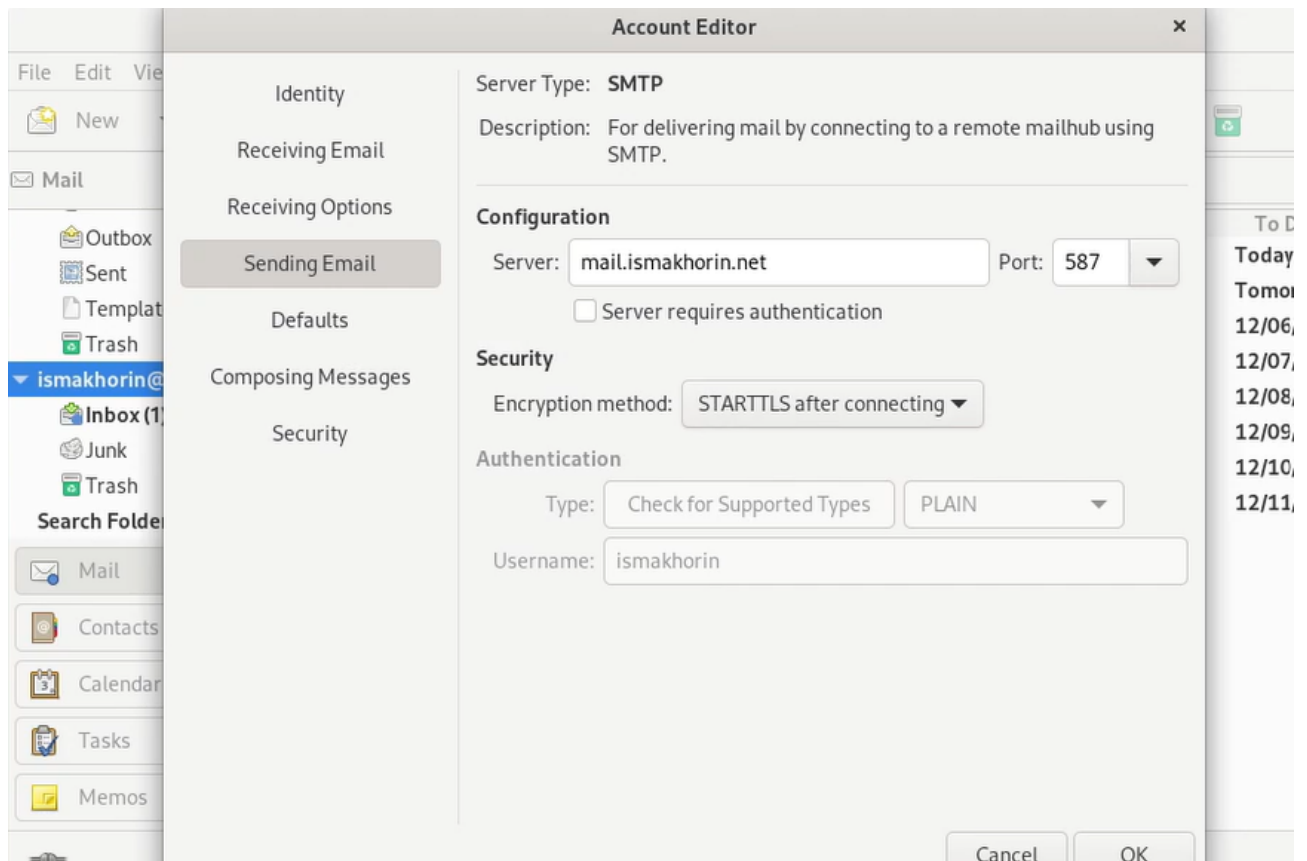
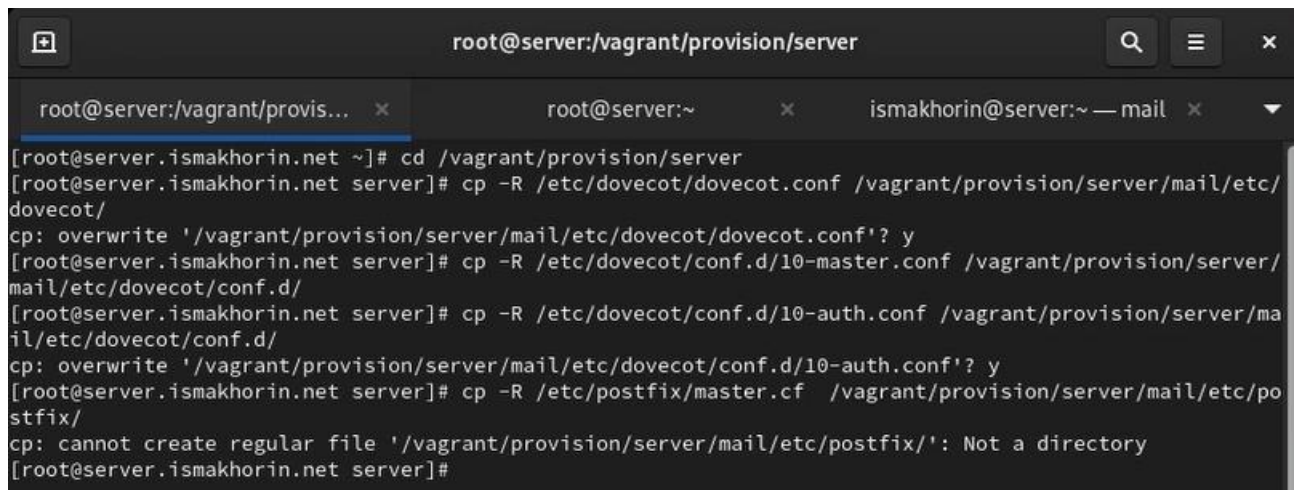


Рис. 3.6. Корректирование настроек почтового клиента Evolution.

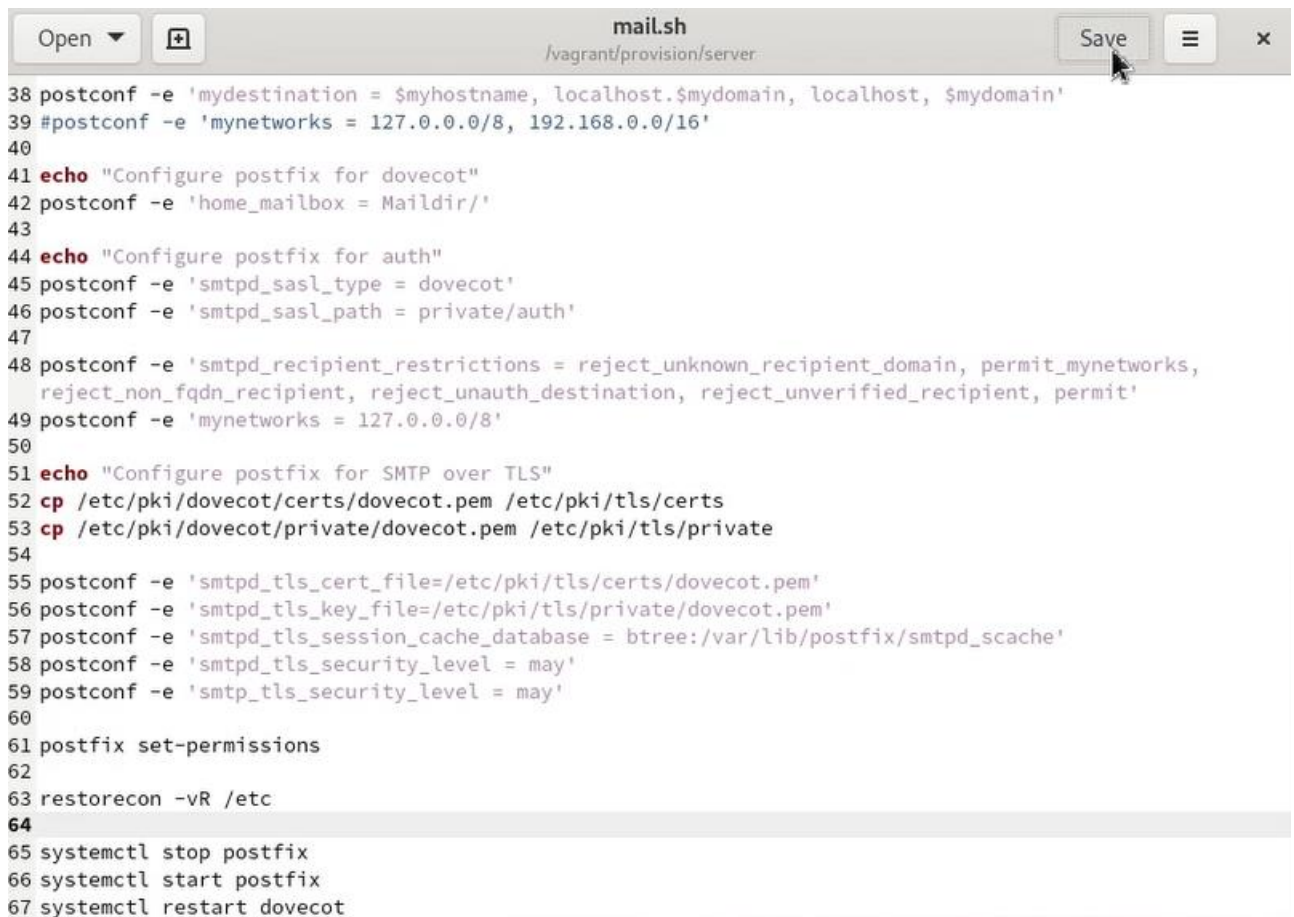
На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`. В соответствующие подкаталоги поместим конфигурационные файлы Dovecot и Postfix (рис. 4.1):



```
root@server:~# cd /vagrant/provision/server
root@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:~# cp -R /etc/dovecot/conf.d/10-master.conf /vagrant/provision/server/mail/etc/dovecot/conf.d/
root@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:~# cp -R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postfix/
cp: cannot create regular file '/vagrant/provision/server/mail/etc/postfix/': Not a directory
root@server:~#
```

Рис. 4.1. Переход в каталог на виртуальной машине server для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и помещение в соответствующие подкаталоги конфигурационных файлов Dovecot и Postfix.

Внесём соответствующие изменения по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh (рис. 4.2):



```
mail.sh
/vagrant/provision/server

38 postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain'
39 #postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'
40
41 echo "Configure postfix for dovecot"
42 postconf -e 'home_mailbox = Maildir/'
43
44 echo "Configure postfix for auth"
45 postconf -e 'smtpd_sasl_type = dovecot'
46 postconf -e 'smtpd_sasl_path = private/auth'
47
48 postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks,
    reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'
49 postconf -e 'mynetworks = 127.0.0.0/8'
50
51 echo "Configure postfix for SMTP over TLS"
52 cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
53 cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
54
55 postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
56 postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
57 postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
58 postconf -e 'smtpd_tls_security_level = may'
59 postconf -e 'smtp_tls_security_level = may'
60
61 postfix set-permissions
62
63 restorecon -vR /etc
64
65 systemctl stop postfix
66 systemctl start postfix
67 systemctl restart dovecot
```

Рис. 4.2. Внесение соответствующих изменений по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh.

Внесём изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet (Рис. 4.3):



```
mail.sh
/vagrant/provision/client

1 #!/bin/bash
2
3 echo "Provisioning script $0"
4
5 echo "Install needed packages"
6 dnf -y install postfix
7 dnf -y install s-nail
8 dnf -y install evolution
9 dnf -y install telnet
10
11 echo "Configure postfix"
12 postconf -e 'inet_protocols = ipv4'
13
14 echo "Start postfix service"
15 systemctl enable postfix
16 systemctl start postfix
```

Рис. 4.3. Внесение изменения в файл /vagrant/provision/client/mail.sh.

Вывод:

В ходе выполнения лабораторной работы были приобретены практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

Ответы на контрольные вопросы:

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

Допустим, у нас есть почтовый ящик с адресом `user@example.com`. В конфигурационном файле Dovecot (`/etc/dovecot/conf.d/10-auth.conf`), мы можем указать формат аутентификации следующим образом:

```
auth_username_format = %Lu
```

В этом примере `%Lu` означает, что аутентификация будет проходить в формате `"user"` без учета регистра букв. Если вам нужно учитывать домен, вы можете использовать `%n`:

```
auth_username_format = %Ln
```

Таким образом, при вводе логина `"user@example.com"` пользователь будет аутентифицироваться с именем пользователя `"user"` и доменом `"example.com"`.

2. Какие функции выполняет почтовый Relay-сервер? –

Пересылка почты: Relay-сервер принимает почтовые сообщения от клиентов и пересылает их к адресатам. Это особенно полезно, если

у вас нет прямого доступа к серверу назначения или если вы хотите централизованно управлять отправкой почты.

Маршрутизация почты: Relay-сервер может определять наилучший маршрут для доставки почты на основе определенных правил и политик.

Блокировка спама: Некоторые Relay-серверы выполняют функции фильтрации спама, блокируя нежелательные сообщения до их отправки на сервер назначения.

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

Открытый Relay: Если сервер настроен как открытый Relay, это может привести к злоупотреблению. Злоумышленники могут использовать сервер для отправки спама, что может повлечь за собой блокировку IP-адреса сервера или другие санкции.

Спуфинг: Атаки, связанные с подделкой отправителя (спуфинг), могут быть использованы для маскировки настоящего источника почты. Это может быть проблемой, если сервер Relay доверяет внешним источникам без должной аутентификации.

Отказ в обслуживании (DoS): Атаки типа DoS могут быть направлены на Relay-сервер, перегружая его запросами на пересылку почты и создавая неприемлемую загрузку.