

Отчёт по лабораторной работе 10

Расширенные настройки SMTP-сервера

Метвалли Ахмед Фарг Набеев

Содержание

1	Цель работы	5
2	Выполнение	6
2.1	Настройка LMTP в Dovecot	6
2.2	Настройка SMTP-аутентификации	10
2.3	Настройка SMTP over TLS	14
3	Выполнение	19
3.1	Внесение изменений в настройки внутреннего окружения виртуальной машины	19
4	Заключение	22
5	Контрольные вопросы	23

Список иллюстраций

2.1	Добавление LMTP в конфигурацию Dovecot	7
2.2	Настройка сервиса lmtp в 10-master.conf	8
2.3	Формат имени пользователя для аутентификации	8
2.4	Отправка тестового письма через LMTP	9
2.5	Фрагмент лога доставки письма	9
2.6	Просмотр почтового ящика пользователя	10
2.7	Конфигурация сервиса аутентификации Dovecot	11
2.8	Настройка SASL в Postfix	11
2.9	Настройки аутентификации в master.cf	13
2.10	Успешная SMTP-аутентификация через Telnet	14
2.11	Настройка параметров TLS в Postfix	14
2.12	Добавление секции submission в master.cf	15
2.13	Проверка TLS-подключения и успешная аутентификация	16
2.14	Настройка SMTP с STARTTLS в почтовом клиенте	17
2.15	Проверка доставки почты через TLS	18
3.1	Копирование конфигурационных файлов Dovecot и Postfix	19
3.2	Обновлённый скрипт конфигурации сервера mail.sh	20
3.3	Изменённый скрипт клиента mail.sh	21

Список таблиц

1 Цель работы

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

2 Выполнение

2.1 Настройка LMTP в Dovecot

1. На виртуальной машине `server` выполнен вход под собственным пользователем и выполнен переход в режим суперпользователя с помощью команды `sudo -i`.
2. В дополнительном терминале запущен мониторинг почтовой службы командой `tail -f /var/log/maillog`.
3. В файле `/etc/dovecot/dovecot.conf` добавлен протокол **LMTP** для поддержки локальной доставки почты.

В результате параметр **protocols** имеет вид:

```
protocols = imap pop3 lmtp
```

```

1 ## Dovecot configuration file
2
3 # If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration
4
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
25 protocols = imap pop3 lmtp
26
27 # A comma separated list of IPs or hosts where to listen in for connections.
28 # "*" listens in all IPv4 interfaces, ":::" listens in all IPv6 interfaces.
29 # If you want to specify non-default ports or anything more complex,
30 # edit conf.d/master.conf.
31 #listen = *, ::

```

Рис. 2.1: Добавление LMTP в конфигурацию Dovecot

4. Для взаимодействия Dovecot с Postfix изменён блок `service lmtp` в файле `/etc/dovecot/conf.d/10-master.conf`.

Новый фрагмент конфигурации задаёт путь к Unix-сокету, права доступа и владельца:



```
43 #port = 995
44 #ssl = yes
45 }
46 }
47
48 service submission-login {
49   inet_listener submission {
50     #port = 587
51   }
52   inet_listener submissions {
53     #port = 465
54   }
55 }
56
57 service lmtp {
58   unix_listener /var/spool/postfix/private/dovecot-lmtp {
59     group = postfix
60     user = postfix
61     mode = 0600
62   }
63 }
64
```

Рис. 2.2: Настройка сервиса lmtp в 10-master.conf

5. В файле `/etc/dovecot/conf.d/10-auth.conf` определён формат имени пользователя для аутентификации без доменной части:

`auth_username_format = %Ln`

```
36 # a character not listed in here, the login automatically fails. this is just
37 # an extra check to make sure user can't exploit any potential quote escaping
38 # vulnerabilities with SQL/LDAP databases. If you want to allow all characters,
39 # set this value to empty.
40 #auth_username_chars = abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890._-@
41
42 # Username character translations before it's looked up from databases. The
43 # value contains series of from -> to characters. For example "#@/@" means
44 # that '#' and '/' characters are translated to '@'.
45 #auth_username_translation =
46
47 # Username formatting before it's looked up from databases. You can use
48 # the standard variables here, eg. %Lu would lowercase the username, %n would
49 # drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
50 # "-AT-". This translation is done after auth_username_translation changes.
51
52 auth_username_format = %Ln
53
54 # If you want to allow master users to log in by specifying the master
55 # username within the normal username string (ie. not using SASL mechanism's
56 # support for it), you can specify the separator character here. The format
57 # is then <username><separator><master username>. UW-IMAP uses "*" as the
58 # separator, so that could be a good choice.
59 #auth_master_user_separator =
60
61 # Username to use for users logging in with ANONYMOUS SASL mechanism
62 #auth_anonymous_username = anonymous
```

Рис. 2.3: Формат имени пользователя для аутентификации

6. В Postfix переопределена доставка сообщений через LMTP-сокеты Dovecot:
`postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'`
7. После изменения конфигурации службы **Postfix** и **Dovecot** были перезапущены:
`systemctl restart postfix`
`systemctl restart dovecot`
8. С клиентской машины отправлено тестовое письмо пользователю:
`echo . | mail -s "LMTP test" ahmedfarg@ahmedfarg.net`

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

Рис. 2.4: Отправка тестового письма через LMTP

9. В логе почтовой службы зафиксирована успешная передача письма от Postfix к Dovecot по протоколу LMTP.
Видно, что сообщение сохранено в почтовом ящике пользователя.

```
Oct 15 09:33:17 server postfix/smtpd[14512]: connect from client.ahmedfarg.net[192.168.1.30]
Oct 15 09:33:17 server postfix/smtpd[14512]: E2891412E535: client=client.ahmedfarg.net[192.168.1.30]
Oct 15 09:33:17 server postfix/cleanup[14516]: E2891412E535: message-id=<20251015093317.CE7CE412ED28@client.ahmedfarg.net>
Oct 15 09:33:17 server postfix/smtpd[14512]: disconnect from client.ahmedfarg.net[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Oct 15 09:33:17 server postfix/qmgr[14234]: E2891412E535: from=<ahmedfarg@client.ahmedfarg.net>, size=554, nrcpt=1 (queue active)
Oct 15 09:33:17 server postfix/local[14517]: E2891412E535: passing <ahmedfarg@ahmedfarg.net> to transport=lmtp
Oct 15 09:33:17 server dovecot[14271]: lmtp(14519): Connect from local
Oct 15 09:33:17 server dovecot[14271]: lmtp(ahmedfarg)<14519><mVuAOF1q72i30AAANsLdkw>: msgid=<20251015093317.CE7CE412ED28@client.ahmedfarg.net>: saved mail to INBOX
Oct 15 09:33:17 server postfix/lmtp[14518]: E2891412E535: to=<ahmedfarg@ahmedfarg.net>, relay=server.ahmedfarg.net [private/dovecot-lmtp], delay=0.04, delays=0/0/0.02/0.01, dsn=2.0.0, status=sent (250 2.0.0 <ahmedfarg@ahmedfarg.net> mVuAOF1q72i30AAANsLdkw Saved)
Oct 15 09:33:17 server dovecot[14271]: lmtp(14519): Disconnect from local: Logged out (state=READY)
Oct 15 09:33:17 server postfix/qmgr[14234]: E2891412E535: removed
```

Рис. 2.5: Фрагмент лога доставки письма

10. На сервере проверено наличие доставленного письма в каталоге Maildir.
Сообщение с темой **"LMTP test"** присутствует в списке писем пользователя.

```
[ahmedfarg@server.ahmedfarg.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.24.  Type '?' for help
/home/ahmedfarg/Maildir: 2 messages 1 new
  1 ahmedfarg          2025-10-11 13:27   18/650   "test
►N  2 ahmedfarg@client.ahm 2025-10-15 09:33   21/838   "LMTP test
& q
Held 2 messages in /home/ahmedfarg/Maildir
[ahmedfarg@server.ahmedfarg.net ~]$ █
```

Рис. 2.6: Просмотр почтового ящика пользователя

2.2 Настройка SMTP-аутентификации

1. В файле `/etc/dovecot/conf.d/10-master.conf` определена служба аутентификации пользователей **auth**.

Этот блок конфигурации обеспечивает взаимодействие между Postfix и Dovecot через Unix-сокеты.

Пояснение:

`service auth` — начало определения службы аутентификации Dovecot.

`unix_listener /var/spool/postfix/private/auth` — создаёт Unix-сокеты для связи Postfix с Dovecot.

`group = postfix` — задаёт группу владельца сокета.

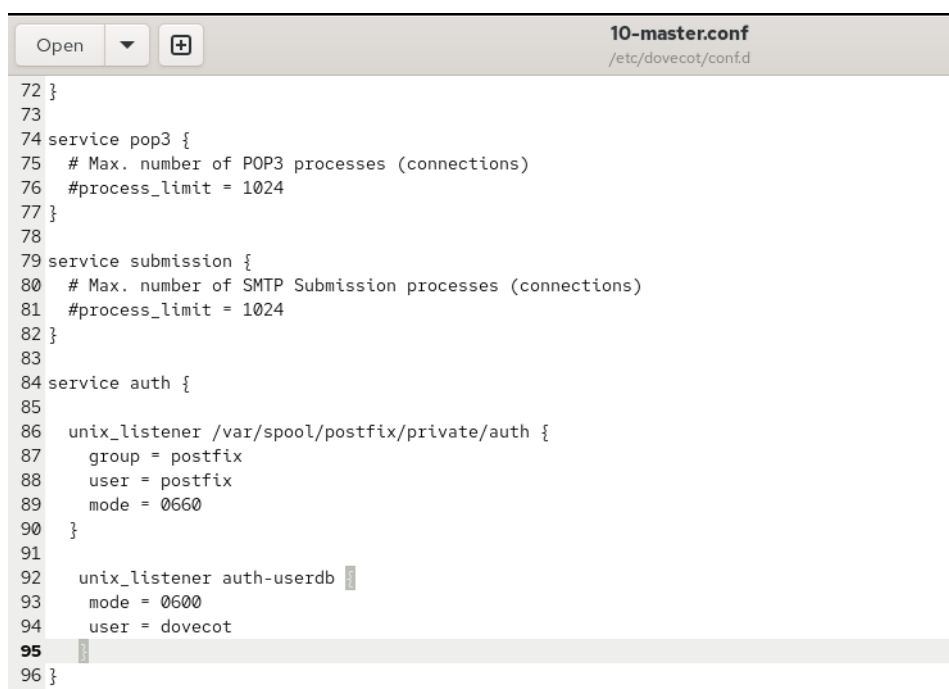
`user = postfix` — определяет пользователя-владельца сокета.

`mode = 0660` — разрешает чтение и запись для владельца и группы.

`unix_listener auth-userdb` — внутренний сокет для взаимодействия Dovecot с базой данных аутентификации.

`mode = 0600` — разрешение только для владельца.

`user = dovecot` — владелец внутреннего сокета — сервис Dovecot.



```
72 }
73
74 service pop3 {
75     # Max. number of POP3 processes (connections)
76     #process_limit = 1024
77 }
78
79 service submission {
80     # Max. number of SMTP Submission processes (connections)
81     #process_limit = 1024
82 }
83
84 service auth {
85
86     unix_listener /var/spool/postfix/private/auth {
87         group = postfix
88         user = postfix
89         mode = 0660
90     }
91
92     unix_listener auth-userdb {
93         mode = 0600
94         user = dovecot
95     }
96 }
```

Рис. 2.7: Конфигурация сервиса аутентификации Dovecot

2. Для Postfix задан тип аутентификации SASL и путь к Unix-сокету, через который осуществляется проверка логинов.

Указано использование Dovecot в качестве механизма SASL и путь `private/auth`.

```
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.ahmedfarg.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.ahmedfarg.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.ahmedfarg.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'
[root@server.ahmedfarg.net ~]#
```

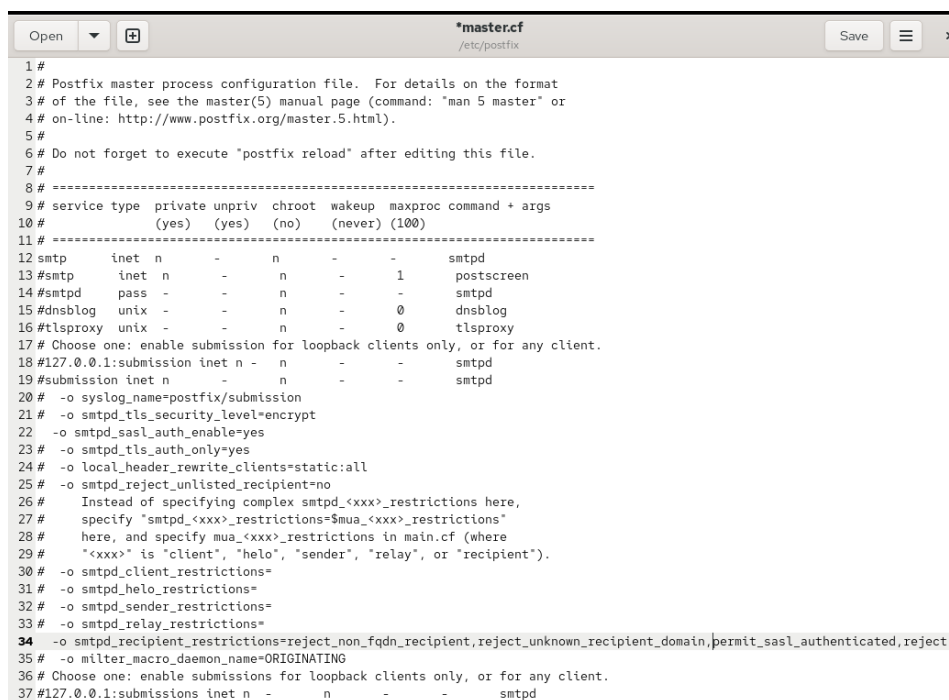
Рис. 2.8: Настройка SASL в Postfix

3. В Postfix настроены ограничения для приёма почты, предотвращающие использование сервера как открытого реляя.

Опция `smtpd_recipient_restrictions` определяет последовательность проверок:

- `reject_unknown_recipient_domain` — отклоняет письма к несуществующим доменам.

- `permit_mynetworks` — разрешает приём писем от доверенных хостов.
 - `reject_non_fqdn_recipient` — блокирует адреса без полного доменного имени.
 - `reject_unauth_destination` — запрещает пересылку на внешние домены.
 - `reject_unverified_recipient` — проверяет существование получателя.
 - `permit` — разрешает приём после успешного прохождения проверок.
4. Для ограничения доступа к серверу почтовые запросы разрешены только с локальной сети.
- В параметре `mynetworks` задан диапазон `127.0.0.0/8`.
5. В файле `/etc/postfix/master.cf` активирована возможность SMTP-аутентификации на порту 25.
- В секции `smtp inet` добавлены параметры включения SASL-аутентификации и ограничений для проверки получателей.



```
1 #
2 # Postfix master process configuration file. For details on the format
3 # of the file, see the master(5) manual page (command: "man 5 master" or
4 # on-line: http://www.postfix.org/master.5.html).
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 # Choose one: enable submission for loopback clients only, or for any client.
18 #127.0.0.1:submission inet n - n - - smtpd
19 #submission inet n - n - - smtpd
20 # -o syslog_name=postfix/submission
21 # -o smtpd_tls_security_level=encrypt
22 # -o smtpd_sasl_auth_enable=yes
23 # -o smtpd_tls_auth_only=yes
24 # -o local_header_rewrite_clients=static:all
25 # -o smtpd_reject_unlisted_recipient=no
26 # Instead of specifying complex smtpd_<xxx>_restrictions here,
27 # specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
28 # here, and specify mua_<xxx>_restrictions in main.cf (where
29 # "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
30 # -o smtpd_client_restrictions=
31 # -o smtpd_helo_restrictions=
32 # -o smtpd_sender_restrictions=
33 # -o smtpd_relay_restrictions=
34 # -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
35 # -o milter_macro_daemon_name=ORIGINATING
36 # Choose one: enable submissions for loopback clients only, or for any client.
37 #127.0.0.1:submissions inet n - n - - smtpd
```

Рис. 2.9: Настройки аутентификации в master.cf

6. После внесённых изменений службы **Postfix** и **Dovecot** были перезапущены.

7. На клиенте установлена утилита **telnet** и сгенерирована строка для аутентификации в формате Base64.

Строка создаётся из логина и пароля пользователя в виде `username username password`.

8. С клиента выполнено подключение к SMTP-серверу по порту 25.

После ввода команды `AUTH PLAIN <строка>` сервер ответил сообщением **235 2.7.0 Authentication successful**, что подтверждает успешную SMTP-аутентификацию.

```
[root@client.ahmedfarg.net ~]#  
[root@client.ahmedfarg.net ~]# printf 'ahmedfarg\x00ahmedfarg\x00123456' | base64  
YWhtZWVmYXJnAGFobWVhZmFyZWxMjM0NTY=  
[root@client.ahmedfarg.net ~]#  
[root@client.ahmedfarg.net ~]#  
[root@client.ahmedfarg.net ~]# telnet server.ahmedfarg.net 25  
Trying 192.168.1.1...  
Connected to server.ahmedfarg.net.  
Escape character is '^J'.  
220 server.ahmedfarg.net ESMTP Postfix  
AUTH PLAIN YWhtZWVmYXJnAGFobWVhZmFyZWxMjM0NTY=  
235 2.7.0 Authentication successful
```

Рис. 2.10: Успешная SMTP-аутентификация через Telnet

2.3 Настройка SMTP over TLS

1. На сервере настроен TLS с использованием временного сертификата Dovecot.

Файлы сертификата и ключа скопированы из каталога `/etc/pki/dovecot` в `/etc/pki/tls/` в соответствующие подкаталоги, чтобы избежать проблем с SELinux.

Далее в конфигурации Postfix указаны пути к файлам сертификата, ключа и каталогу для хранения TLS-сессий, а также определён уровень безопасности для зашифрованных соединений.

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

Рис. 2.11: Настройка параметров TLS в Postfix

2. Для запуска SMTP-сервера на порту 587 в файле `/etc/postfix/master.cf` добавлена секция **submission**.

Она обеспечивает поддержку TLS и SASL-аутентификации, а также задаёт

ограничения для проверки получателей.

Настройка секции выглядит следующим образом:

- `submission inet n - n - - smtpd` — активация службы SMTP Submission.
- `-o smtpd_tls_security_level=encrypt` — обязательное шифрование соединений.
- `-o smtpd_sasl_auth_enable=yes` — включение аутентификации.
- `-o smtpd_recipient_restrictions=...` — правила приёма сообщений.

```
1 #
2 # Postfix master process configuration file. For details on the format
3 # of the file, see the master(5) manual page (command: "man 5 master" or
4 # on-line: http://www.postfix.org/master.5.html).
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 # Choose one: enable submission for loopback clients only, or for any client.
18 #127.0.0.1:submission inet n - n - - smtpd
19 submission inet n       -       n       -       -       smtpd
20 # -o syslog_name=postfix/submission
21 # -o smtpd_tls_security_level=encrypt
22 # -o smtpd_sasl_auth_enable=yes
23 # -o smtpd_tls_auth_only=yes
24 # -o local_header_rewrite_clients=static:all
25 # -o smtpd_reject_unlisted_recipient=no
26 #   Instead of specifying complex smtpd_<xxx>_restrictions here,
27 #   specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
28 #   here, and specify mua_<xxx>_restrictions in main.cf (where
29 #   "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
30 # -o smtpd_client_restrictions=
31 # -o smtpd_helo_restrictions=
32 # -o smtpd_sender_restrictions=
33 # -o smtpd_relay_restrictions=
34 # -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
35 # -o milter_macro_daemon_name=ORIGINATING
36 # Choose one: enable submissions for loopback clients only, or for any client.
37 #127.0.0.1:submissions inet n - n - - smtpd
```

Рис. 2.12: Добавление секции submission в master.cf

3. В межсетевом экране разрешена работа службы **smtp-submission**.

Это обеспечивает доступ к порту 587 как временно, так и на постоянной основе после перезапуска системы.

4. После внесения изменений служба **Postfix** была перезапущена для применения новых параметров конфигурации.

5. С клиентской машины выполнено подключение к SMTP-серверу через порт 587 с использованием `openssl`.

Проверка показала корректную работу TLS-соединения и успешную SMTP-аутентификацию пользователя.

Сервер ответил сообщением **235 2.7.0 Authentication successful**, что подтверждает защищённое подключение и успешную проверку учётных данных.

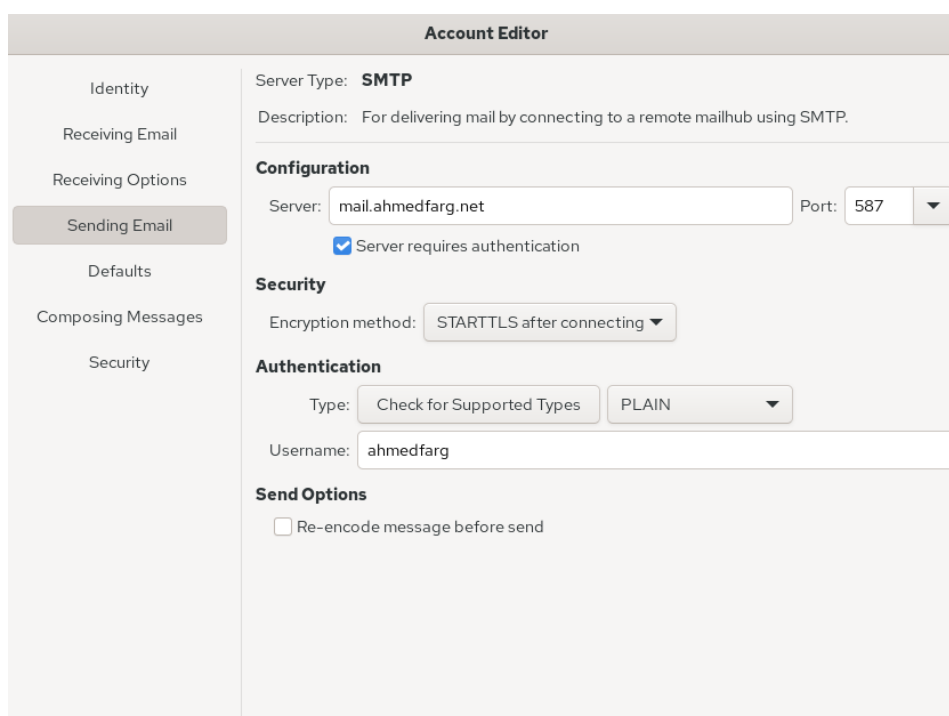
```
Start Time: 1760522671
Timeout   : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
EHLO test
250-server.ahmedfarg.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN YWhtZWRmYXJnAGFobWVkJmFyZWAxMjM0NTY=
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
closed
[root@client.ahmedfarg.net ~]#
```

Рис. 2.13: Проверка TLS-подключения и успешная аутентификация

6. В почтовом клиенте **Evolution** внесены изменения в настройки отправки почты.

Для SMTP-сервера указан порт **587**, метод шифрования **STARTTLS after connecting** и тип аутентификации **PLAIN**.

Пользователь вводит логин для проверки подлинности при отправке писем.



The screenshot shows the 'Account Editor' window with a sidebar on the left containing the following menu items: Identity, Receiving Email, Receiving Options, Sending Email (highlighted), Defaults, Composing Messages, and Security. The main panel is titled 'SMTP' and includes a description: 'For delivering mail by connecting to a remote mailhub using SMTP.' Below this, the 'Configuration' section contains a 'Server' field with 'mail.ahmedfarg.net' and a 'Port' dropdown set to '587'. A checkbox 'Server requires authentication' is checked. The 'Security' section shows an 'Encryption method' dropdown set to 'STARTTLS after connecting'. The 'Authentication' section has a 'Type' dropdown with 'Check for Supported Types' and 'PLAIN' (selected), and a 'Username' field with 'ahmedfarg'. The 'Send Options' section at the bottom has an unchecked checkbox 'Re-encode message before send'.

Рис. 2.14: Настройка SMTP с STARTTLS в почтовом клиенте

7. Отправка почтовых сообщений с клиента успешно проверена.

Входящие письма отображаются в папке **Inbox**, что подтверждает корректную работу SMTP over TLS и шифрованную доставку сообщений.

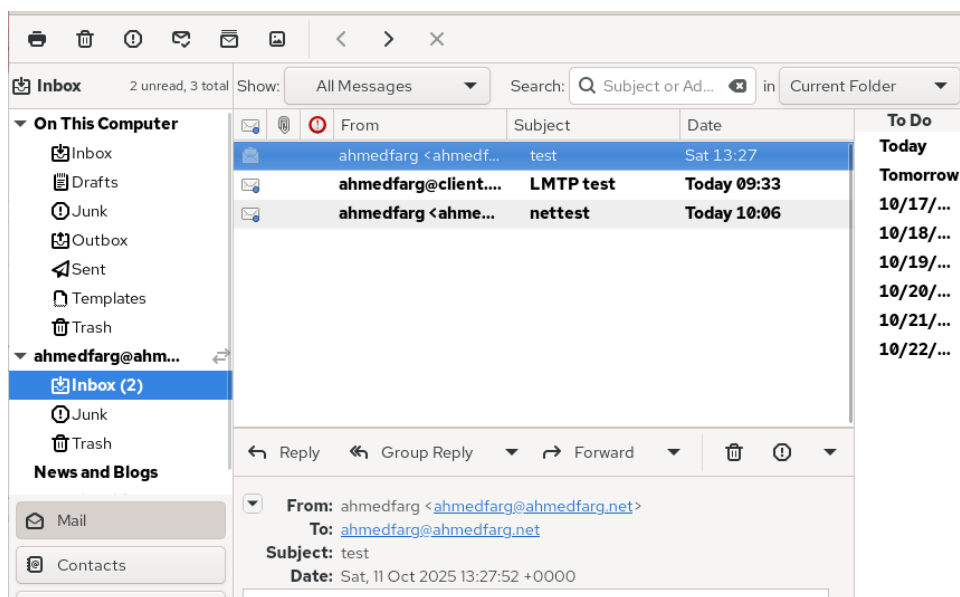


Рис. 2.15: Проверка доставки почты через TLS

3 Выполнение

3.1 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине `server` выполнен переход в каталог `/vagrant/provision/server/` для внесения изменений в настройки окружения.

В соответствующие подкаталоги помещены конфигурационные файлы **Dovecot** и **Postfix**.

```
[root@server.ahmedfarg.net ~]#  
[root@server.ahmedfarg.net ~]# cd /vagrant/provision/server/  
[root@server.ahmedfarg.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.ahmedfarg.net server]# cp -R /etc/dovecot/conf.d/10-master.conf /vagrant/provision/server/mail/etc/dovecot/conf.d/  
[root@server.ahmedfarg.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.ahmedfarg.net server]#  
[root@server.ahmedfarg.net server]# mkdir -p /vagrant/provision/server/mail/etc/postfix  
[root@server.ahmedfarg.net server]# cp -R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postfix  
[root@server.ahmedfarg.net server]#
```

Рис. 3.1: Копирование конфигурационных файлов Dovecot и Postfix

2. В файл `/vagrant/provision/server/mail.sh` внесены изменения для расширенной конфигурации SMTP-сервера.

```

4  dnf -y install postfix
5  dnf -y install dovecot
6  dnf -y install telnet
7  echo "Copy configuration files"
8  cp -R /vagrant/provision/server/mail/etc/* /etc
9  chown -R root:root /etc/postfix
10 restorecon -vR /etc
11 echo "Configure firewall"
12 firewall-cmd --add-service smtp --permanent
13 firewall-cmd --add-service pop3 --permanent
14 firewall-cmd --add-service pop3s --permanent
15 firewall-cmd --add-service imap --permanent
16 firewall-cmd --add-service imaps --permanent
17 firewall-cmd --add-service smtp-submission --permanent
18 firewall-cmd --reload
19 echo "Start postfix service"
20 systemctl enable postfix
21 systemctl start postfix
22 echo "Configure postfix"
23 postconf -e 'mydomain = ahmedfarg.net'
24 postconf -e 'myorigin = $mydomain'
25 postconf -e 'inet_protocols = ipv4'
26 postconf -e 'inet_interfaces = all'
27 postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain'
28 #postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'
29 echo "Configure postfix for dovecot"
30 postconf -e 'home_mailbox = Maildir/'
31 echo "Configure postfix for auth"
32 postconf -e 'smtpd_sasl_type = dovecot'
33 postconf -e 'smtpd_sasl_path = private/auth'
34 postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks'
35 postconf -e 'mynetworks = 127.0.0.0/8'
36 echo "Configure postfix for SMTP over TLS"
37 cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
38 cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
39 postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
40 postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
41 postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
42 postconf -e 'smtpd_tls_security_level = may'
43 postconf -e 'smtp_tls_security_level = may'
44 postfix set-permissions
45 restorecon -vR /etc
46 systemctl stop postfix

```

Рис. 3.2: Обновлённый скрипт конфигурации сервера mail.sh

- В файл /vagrant/provision/client/mail.sh добавлена установка пакета telnet и почтового клиента evolution, необходимых для тестирования и проверки работы SMTP-сервера.

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

Рис. 3.3: Изменённый скрипт клиента mail.sh

4 Заключение

SMTP-сервер был успешно настроен для работы с безопасной аутентификацией и шифрованием с использованием TLS.

Dovecot и Postfix интегрированы через LMTP и SASL, что обеспечивает корректную доставку и защищённую передачу почты.

5 Контрольные вопросы

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

Формат указывается в параметре `auth_username_format`, например:

```
auth_username_format = %n%d
```

где `%n` — имя пользователя, а `%d` — домен (например, `user@example.com`).

2. **Какие функции выполняет почтовый Relay-сервер?**

Relay-сервер (посредник) принимает почту от одного почтового узла и пересылает её другому серверу, выступая промежуточным звеном между отправителем и конечным получателем.

Основные функции — маршрутизация сообщений, передача писем между доменами и поддержка внешних соединений при отправке почты.

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

Если почтовый сервер настроен как открытый релей (Open Relay), он может быть использован злоумышленниками для рассылки спама и фишинговых писем.

Это приведёт к блокировке IP-адреса сервера, попаданию в «чёрные списки» и снижению доверия к почтовому домену.

Также возможно увеличение нагрузки и утечка конфиденциальных данных при отсутствии аутентификации и шифрования.