

Отчёт по лабораторной работе 10

Расширенные настройки SMTP-сервера

Элсаиед Адел

Содержание

1 Цель работы	5
2 Выполнение	6
2.1 Настройка LMTP и SMTP-аутентификации в Dovecot и Postfix	6
2.2 Настройка SMTP-аутентификации	9
2.3 Настройка SMTP over TLS	12
2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины	16
3 Вывод	18
4 Контрольные вопросы	19

Список иллюстраций

2.1 Добавление протокола LMTP в dovecot.conf	7
2.2 Настройка сервиса LMTP в Dovecot	7
2.3 Настройка формата имени пользователя	8
2.4 Журнал доставки письма через LMTP	8
2.5 Проверка почтового ящика пользователя	9
2.6 Настройка службы auth в Dovecot	10
2.7 Настройка SASL-аутентификации в Postfix	10
2.8 Изменение master.cf для тестирования SMTP AUTH	11
2.9 Проверка SMTP-аутентификации через telnet	12
2.10 Копирование сертификата и ключа Dovecot для TLS	12
2.11 Настройка master.cf для SMTP over TLS	13
2.12 Проверка SMTP over TLS через openssl	14
2.13 Отправка почты через Evolution по TLS	15
2.14 Журнал доставки письма по SMTP over TLS	15
2.15 Копирование конфигурационных файлов в каталог provision	16
2.16 Изменения в provisioning-скрипте mail.sh на сервере	17
2.17 Изменения в provisioning-скрипте mail.sh на клиенте	17

Список таблиц

1 Цель работы

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

2 Выполнение

2.1 Настройка LMTP и SMTP-аутентификации в Dovecot и Postfix

1. На виртуальной машине **server** был выполнен вход под учётной записью пользователя с последующим переходом в режим суперпользователя. Это необходимо для внесения изменений в системные конфигурационные файлы почтовых сервисов.
2. В отдельном терминальном окне был запущен мониторинг журнала работы почтовой службы. Файл `/var/log/maillog` используется для отслеживания процессов приёма, передачи и доставки почты, а также для анализа взаимодействия Postfix и Dovecot в режиме реального времени.
3. В конфигурационном файле `/etc/dovecot/dovecot.conf` был изменён список поддерживаемых протоколов. В параметр `protocols` добавлен протокол LMTP, что позволяет Dovecot принимать почтовые сообщения от Postfix по локальному протоколу доставки.

```

dovecot.conf
/etc/dovecot
5 # "doveconf -n" command gives a clean output of the changed settings. Use it
l 6 # instead of copy&pasting files when posting to the Dovecot mailing list.
t 7
t 8 #' character and everything after it is treated as comments. Extra spaces
t 9 # and tabs are ignored. If you want to use either of these explicitly, put the
t 10 # value inside quotes, eg.: key = "# char and trailing whitespace "
t 11
t 12 # Most (but not all) settings can be overridden by different protocols and/or
t 13 # source/destination IPs by placing the settings inside sections, for example:
t 14 # protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }
e 15
t 16 # Default values are shown for each setting, it's not required to uncomment
e 17 # those. These are exceptions to this though: No sections (e.g. namespace {})
t 18 # or plugin settings are added by default, they're listed only as examples.
e 19 # Paths are also just examples with the real defaults being based on configuration
t 20 # options. The paths listed here are for configure --prefix=/usr
e 21 # --sysconfdir=/etc --localstatedir=/var
t 22
e 23 # Protocols we want to be serving.
t 24
p 25 protocols = imap pop3 lmtp
t 26

```

Рис. 2.1: Добавление протокола LMTP в dovecot.conf

4. Для организации связи между Postfix и Dovecot по протоколу LMTP был настроен сервис lmtp в файле /etc/dovecot/conf.d/10-master.conf. В конфигурации определён UNIX-сокет /var/spool/postfix/private/dovecot-lmtp, принадлежащий пользователю и группе postfix с правами доступа 0600. Это обеспечивает безопасный локальный обмен почтовыми сообщениями.

```

10-master.conf
/etc/dovecot/conf.d
52 inet_listener submission {
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     # Create inet listener only if you can't use the above UNIX socket
65     #inet_listener lmtp {
66         # Avoid making LMTP visible for the entire internet
67         #address =
68         #port =
69     }
70
71

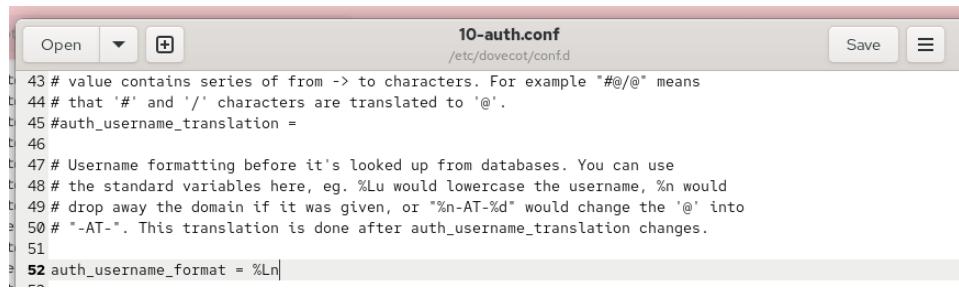
```

Рис. 2.2: Настройка сервиса LMTP в Dovecot

5. В Postfix была изменена схема доставки почты. Передача сообщений в почтовый ящик пользователя была настроена через LMTP с использовани-

ем ранее созданного UNIX-сокета, что позволяет Postfix передавать почту Dovecot не напрямую, а через локальный механизм доставки.

6. В файле `/etc/dovecot/conf.d/10-auth.conf` был задан формат имени пользователя для аутентификации. Использование параметра `auth_username_format = %Ln` обеспечивает работу с логином пользователя без доменной части и приведение имени к нижнему регистру.



```
Open + 10-auth.conf /etc/dovecot/conf.d Save =  
b 43 # value contains series of from -> to characters. For example "#@/" means  
b 44 # that '#' and '/' characters are translated to '@'.  
b 45 #auth_username_translation =  
b 46  
b 47 # Username formatting before it's looked up from databases. You can use  
b 48 # the standard variables here, eg. %Lu would lowercase the username, %n would  
b 49 # drop away the domain if it was given, or "%n-AT-%d" would change the "@" into  
b 50 # "-AT-". This translation is done after auth_username_translation changes.  
b 51  
b 52 auth_username_format = %Ln  
--
```

Рис. 2.3: Настройка формата имени пользователя

7. После внесения изменений конфигурационные файлы были применены путём перезапуска сервисов Postfix и Dovecot.
8. Из-под учётной записи пользователя на клиентской машине было отправлено тестовое письмо. В процессе мониторинга журнала `/var/log/maillog` зафиксированы этапы SMTP-сеанса, передача сообщения по LMTP и его успешная доставка в почтовый ящик пользователя. Это подтверждает корректную работу механизма LMTP.



```
Jan 4 09:01:36 server postfix/smtpd[28168]: warning: run-time library vs. compile-time header version mismatch: OpenSSL 3.5.0 may not be compatible with OpenSSL 3.2.0  
Jan 4 09:01:36 server postfix/smtpd[28168]: connect from client.elsaiedadel.net[192.168.1.30]  
Jan 4 09:01:36 server postfix/smtpd[28168]: client=smtpd[28168]: client=client.elsaiedadel.net[192.168.1.30]  
Jan 4 09:01:36 server postfix/cleanup[28172]: 5A1D3205D7F8: message-id=<20260104090136.4F1EB412EDBE@client.elsaiedadel.net>  
Jan 4 09:01:36 server postfix/smtpd[28168]: disconnect from client.elsaiedadel.net[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7  
Jan 4 09:01:36 server postfix/qmgr[28026]: 5A1D3205D7F8: from=<elsaiedadel@client.elsaiedadel.net>, size=576, nrcpt=1 (queue active )  
Jan 4 09:01:36 server postfix/local[28173]: 5A1D3205D7F8: passing <elsaiedadel@elsaiedadel.net> to transport=lmtp  
Jan 4 09:01:36 server dovecot[28062]: lmtp(28175): Connect from local  
Jan 4 09:01:36 server dovecot[28062]: lmtp(elsaiedadel)<28175><T1e9FnAsWmkPbgAA6DgeiQ>: msgid=<20260104090136.4F1EB412EDBE@client.elsaiedadel.net>; saved mail to INBOX  
Jan 4 09:01:36 server postfix/lmtp[28174]: 5A1D3205D7F8: to=<elsaiedadel@elsaiedadel.net>, relay=server.elsaiedadel.net[private/dovecot-lmtp], delay=0.02, delays=0/0/0.01, dsn=2.0.0, status=sent (250 2.0.0 <elsaiedadel@elsaiedadel.net> T1e9FnAsWmkPbgAA6DgeiQ Saved)  
Jan 4 09:01:36 server dovecot[28062]: lmtp(28175): Disconnect from local: Logged out (state=READY)  
Jan 4 09:01:36 server postfix/qmgr[28026]: 5A1D3205D7F8: removed
```

Рис. 2.4: Журнал доставки письма через LMTP

9. На сервере был просмотрен почтовый ящик пользователя в формате Maildir. В списке сообщений обнаружено тестовое письмо с темой *LMDTP test*, что подтверждает успешную доставку сообщения.

```
[elsaiedadel@server.elsaiedadel.net named]$  
[elsaiedadel@server.elsaiedadel.net named]$ MAIL=~/Maildir/ mail  
s-nail version v14.9.24. Type `?' for help  
/home/elsaiedadel/Maildir: 2 messages 1 new  
  1 elsaiedadel 2026-01-04 08:43 18/684 "test1"  
►N 2 elsaiedadel@client.e 2026-01-04 09:01 21/880 "LMDTP test"  
& q  
Held 2 messages in /home/elsaiedadel/Maildir  
[elsaiedadel@server.elsaiedadel.net named]$ █
```

Рис. 2.5: Проверка почтового ящика пользователя

2.2 Настройка SMTP-аутентификации

1. В файле `/etc/dovecot/conf.d/10-master.conf` была настроена служба auth. UNIX-сокет `/var/spool/postfix/private/auth` используется Postfix для выполнения SMTP-аутентификации через Dovecot и принадлежит пользователю и группе `postfix` с правами 0660.
Сокет `auth-userdb` предназначен для внутренних нужд Dovecot и обеспечивает доступ к базе пользователей, работая от имени пользователя `dovecot` с правами 0600.

```

85
86 service submission {
87     # Max. number of SMTP Submission processes (connections)
88     #process_limit = 1024
89 }
90
91 service auth {
92     unix_listener auth-userdb {
93         mode = 0600
94         user = dovecot
95     }
96
97     unix_listener /var/spool/postfix/private/auth {
98         group = postfix
99         user = postfix
100        mode = 0660
101    }
102
103 }
104

```

Рис. 2.6: Настройка службы auth в Dovecot

2. В Postfix был задан тип SASL-аутентификации и путь к UNIX-сокету Dovecot. Это позволило SMTP-серверу использовать механизмы аутентификации Dovecot при приёме почтовых сообщений от клиентов.

```

[root@server.elsatedadel.net server]#
[root@server.elsatedadel.net server]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.elsatedadel.net server]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.elsatedadel.net server]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_my networks
, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'
[root@server.elsatedadel.net server]# postconf -e 'my networks = 127.0.0.0/8'
[root@server.elsatedadel.net server]#

```

Рис. 2.7: Настройка SASL-аутентификации в Postfix

3. Для предотвращения использования сервера в качестве SMTP relay была настроена цепочка ограничений `smtpd_recipient_restrictions`. Указанные параметры обеспечивают отклонение некорректных адресов, запрет пересылки почты для неавторизованных доменов, а также разрешение доставки для доверенных сетей и аутентифицированных пользователей.
4. В параметре `my networks` был ограничен приём почты только с локального адресного пространства `127.0.0.0/8`, что дополнительно повышает уровень безопасности SMTP-сервера.

5. Для проверки работы SMTP-аутентификации в файле `/etc/postfix/master.cf` был временно включён SMTP-сервис с поддержкой SASL-аутентификации. Это позволило выполнить тестирование механизма авторизации без использования защищённого соединения.

```

master.cf
/etc/postfix

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
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
38 #submissions  inet n      -      n      -      -      smtpd

```

Рис. 2.8: Изменение master.cf для тестирования SMTP AUTH

6. На клиентской машине была установлена утилита telnet. После генерации строки аутентификации в формате base64 было выполнено подключение к SMTP-серверу по порту 25. В ходе тестирования подтверждено наличие механизма AUTH PLAIN, а успешная авторизация пользователя свидетельствует о корректной настройке SMTP-аутентификации.

```

[root@client.elsaiedadel.net client]#
[root@client.elsaiedadel.net client]# printf 'elsaiedadel\x00elsaiedadel\x00123456' | base64
ZWxzYWllZGFkZWwAZWxzYWllZGFkZWwAMTIzNDU2
[root@client.elsaiedadel.net client]# telnet server.elsaiedadel.net 25
Trying 192.168.1.1...
Connected to server.elsaiedadel.net.
Escape character is '^].
220 server.elsaiedadel.net ESMTP Postfix
EHLO test
250-server.elsaiedadel.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 ZWxzYWllZGFkZWwAZWxzYWllZGFkZWwAMTIzNDU2
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
Connection closed by foreign host.
[root@client.elsaiedadel.net client]#

```

Рис. 2.9: Проверка SMTP-аутентификации через telnet

2.3 Настройка SMTP over TLS

- На виртуальной машине **server** была выполнена настройка поддержки TLS для SMTP с использованием временного самоподписанного сертификата Dovecot. Во избежание проблем с SELinux сертификат и закрытый ключ были предварительно скопированы из каталога `/etc/pki/dovecot` в стандартные каталоги TLS `/etc/pki/tls/certs` и `/etc/pki/tls/private`.

```

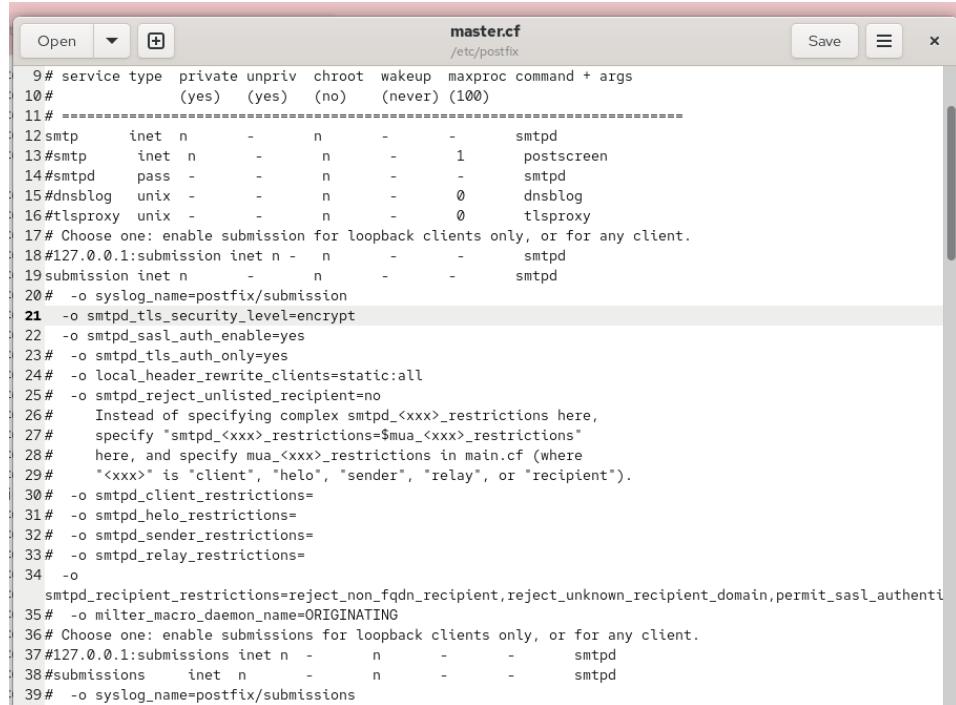
-----
[root@server.elsaiedadel.net server]#
[root@server.elsaiedadel.net server]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs/
[root@server.elsaiedadel.net server]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private/
[root@server.elsaiedadel.net server]# postconf -e 'smtpd_tls_cert_file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

```

Рис. 2.10: Копирование сертификата и ключа Dovecot для TLS

- В конфигурации Postfix были заданы пути к TLS-сертификату и ключу, а также настроено хранилище кэша TLS-сессий и уровень безопасности. Уровень `may` разрешает использование шифрования при поддержке его клиентом, не делая TLS обязательным для всех соединений.

3. Для разделения обычного SMTP и SMTP over TLS была изменена конфигурация файла `/etc/postfix/master.cf`. Основной SMTP-сервис оставлен без принудительного шифрования, а для службы `submission` (порт 587) включено обязательное использование TLS и SMTP-аутентификации. Это соответствует общепринятой практике безопасной отправки почты клиентами.



```

master.cf
/etc/postfix

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", "hello", "sender", "relay", or "recipient").
30 # -o smtpd_client_restrictions=
31 # -o smtpd_hello_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
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
38 #submissions  inet n - n - - smtpd
39 # -o syslog_name=postfix/submissions

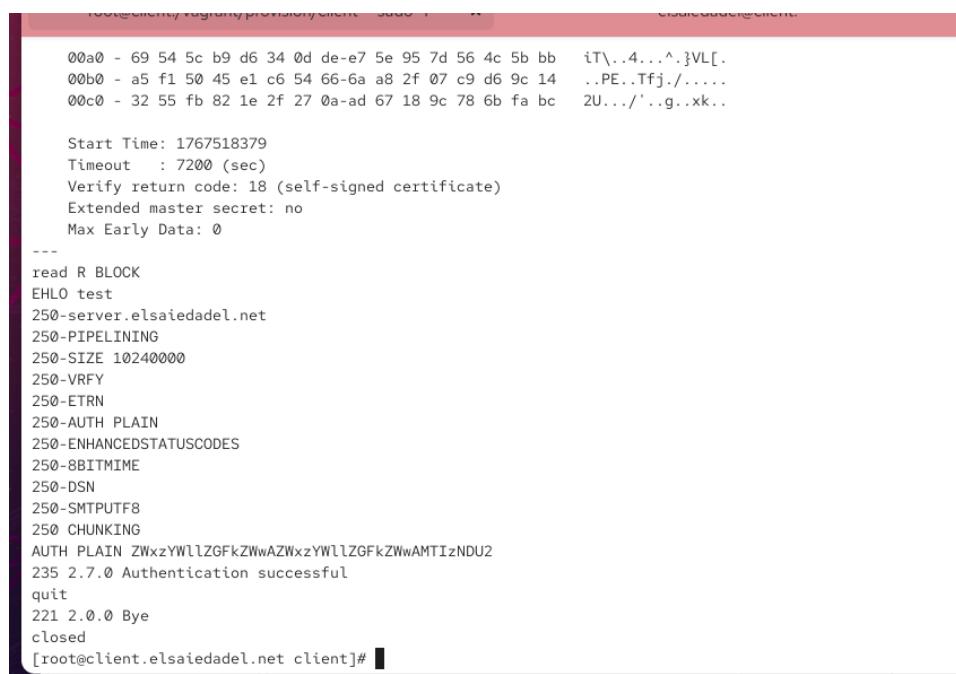
```

Рис. 2.11: Настройка master.cf для SMTP over TLS

4. На сервере был настроен межсетевой экран: разрешена служба `smtp-submission`, обеспечивающая приём почты по порту 587. После внесения изменений конфигурация `firewall` была перезагружена для применения правил.
5. Почтовая служба Postfix была перезапущена, что позволило применить все изменения, связанные с TLS и портом `submission`.
6. На клиентской виртуальной машине было выполнено подключение к SMTP-серверу по порту 587 с использованием STARTTLS через `openssl`. В ходе

сеанса подтверждено установление TLS-соединения, использование само-подписанного сертификата и успешное объявление сервером механизмов аутентификации.

После выполнения команды EHLO сервер сообщил о поддержке AUTH PLAIN, а успешная аутентификация пользователя подтвердила корректность настройки SMTP over TLS.



```
root@client:~$ openssl s_client -connect 250-server.elsaiedadel.net:25 -starttls smtp -crlf -quiet
CONNECTED(00000003)
depth=2 C = EG, O = Internet Solutions, CN = Internet Solutions Root CA
depth=1 C = EG, O = Internet Solutions, CN = Internet Solutions CA-1
depth=0 C = EG, O = Internet Solutions, CN = 250-server.elsaiedadel.net
verify return:1
depth=2 C = EG, O = Internet Solutions, CN = Internet Solutions Root CA
depth=1 C = EG, O = Internet Solutions, CN = Internet Solutions CA-1
depth=0 C = EG, O = Internet Solutions, CN = 250-server.elsaiedadel.net
-----
```

00a0 - 69 54 5c b9 d6 34 0d de-e7 5e 95 7d 56 4c 5b bb iT\..4...^.{VL[.
00b0 - a5 f1 50 45 e1 c6 54 66-6a a8 2f 07 c9 d6 9c 14 ..PE..Tfj./.....
00c0 - 32 55 fb 82 1e 2f 27 0a-ad 67 18 9c 78 6b fa bc 2U.../'..g..xk...

Start Time: 1767518379
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.elsaiedadel.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITTIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN ZWxzYWllZGFkZWwAZWxzYWllZGFkZWwAMTIzNDU2
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
closed
[root@client.elsaiedadel.net client]#

Рис. 2.12: Проверка SMTP over TLS через openssl

7. Корректность отправки почтовых сообщений была дополнительно проверена с использованием почтового клиента **Evolution**. В настройках учётной записи для SMTP-сервера были указаны порт 587, метод шифрования STARTTLS и обычный пароль пользователя. Отправленные письма были успешно доставлены в почтовый ящик.

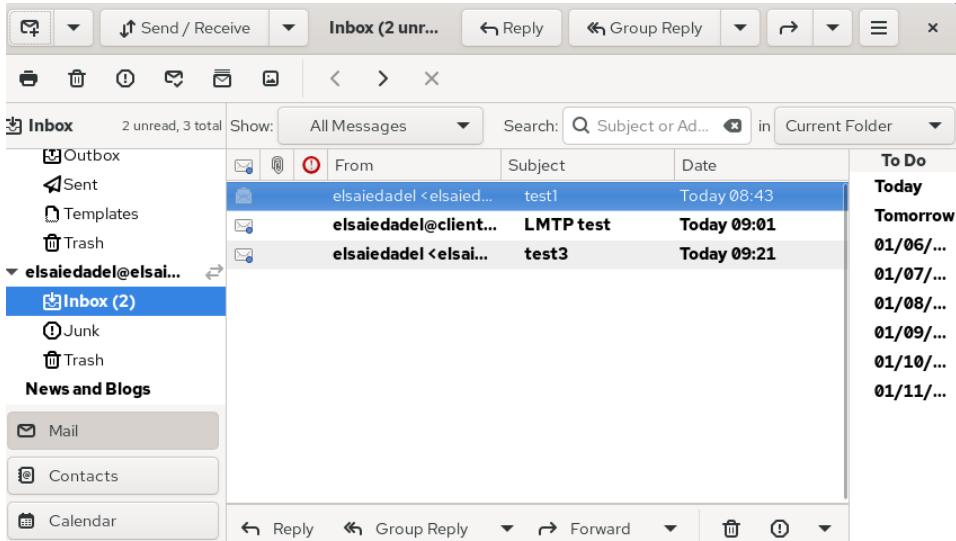


Рис. 2.13: Отправка почты через Evolution по TLS

8. В журнале `/var/log/maillog` зафиксированы этапы TLS-сессии, SMTP-аутентификация пользователя и передача сообщения по LMTP в Dovecot с последующей доставкой в почтовый ящик. Это подтверждает корректную работу всей цепочки: SMTP over TLS → SASL-аутентификация → LMTP-доставка.

```

Jan 4 09:21:10 server postfix/smtpd[31073]: connect from client.elsaiedadel.net[192.168.1.30]
Jan 4 09:21:10 server postfix/tlsmgr[30912]: warning: btree:/var/lib/postfix/smtpd_scache is unavailable. unsupported dictionary type: btree
Jan 4 09:21:15 server postfix/smtpd[31073]: 1D218205D7F8: client=client.elsaiedadel.net[192.168.1.30], sasl_method=PLAIN, sasl_user
name=elsaiedadel
Jan 4 09:21:15 server postfix/cleanup[31314]: 1D218205D7F8: message-id=<7c8dee44bed567e0b13af804043dfa94a6a0a2e1.camel@elsaiedadel.
net>
Jan 4 09:21:15 server postfix/qmgr[30908]: 1D218205D7F8: from=<elsaiedadel@elsaiedadel.net>, size=572, nrcpt=1 (queue active)
Jan 4 09:21:15 server postfix/smtpd[31073]: disconnect from client.elsaiedadel.net[192.168.1.30] ehlo=2 starttls=1 auth=1 mail=1 rc
pt=1 data=1 quit=1 commands=8
Jan 4 09:21:15 server postfix/local[31315]: 1D218205D7F8: passing <elsaiedadel@elsaiedadel.net> to transport=lmtp
Jan 4 09:21:15 server dovecot[29598]: lmtp(31317): Connect from local
Jan 4 09:21:15 server dovecot[29598]: lmtp(elsaiedadel)<31317><p/XZBwsxWmlVegAA6DgeiQ>: msgid=<7c8dee44bed567e0b13af804043dfa94a6a0
a2e1.camel@elsaiedadel.net>; saved mail to INBOX
Jan 4 09:21:15 server postfix/lmtp[31316]: 1D218205D7F8: to=<elsaiedadel@elsaiedadel.net>, relay=server.elsaiedadel.net[private/dov
ecot-lmtp], delay=0.02, delays=0.01/0/0.01/0, dsn=2.0.0, status=sent (250 2.0.0 <elsaiedadel@elsaiedadel.net> p/XZBwsxWmlVegAA6DgeiQ
Saved)
Jan 4 09:21:15 server dovecot[29598]: lmtp(31317): Disconnect from local: Logged out (state=READY)
Jan 4 09:21:15 server postfix/qmgr[30908]: 1D218205D7F8: removed

```

Рис. 2.14: Журнал доставки письма по SMTP over TLS

2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

9. Для сохранения конфигурации почтового сервера в системе автоматизированного развёртывания Vagrant на виртуальной машине **server** был выполнен переход в каталог `/vagrant/provision/server`. В соответствующие подкаталоги были скопированы актуальные конфигурационные файлы Dovecot и Postfix.

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

Рис. 2.15: Копирование конфигурационных файлов в каталог provision

10. В файл `/vagrant/provision/server/mail.sh` были внесены изменения, обеспечивающие автоматическую установку необходимых пакетов, копирование конфигурационных файлов, настройку межсетевого экрана, включение и запуск Postfix, а также полную конфигурацию Postfix для работы с Dovecot, SMTP-аутентификацией и SMTP over TLS. Это позволяет при повторном развёртывании виртуальной машины автоматически получать полностью настроенный почтовый сервер.

```

#!/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 = elsaiedadel.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'

```

Рис. 2.16: Изменения в provisioning-скрипте mail.sh на сервере

11. В provisioning-скрипт клиента /vagrant/provision/client/mail.sh была добавлена установка утилиты telnet. Это необходимо для возможности проверки SMTP-соединений и аутентификации с клиентской стороны после автоматического развёртывания виртуальной машины.

```

#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install postfix
dnf -y install s-nail evolution telnet
echo "Configure postfix"
postconf -e 'inet_protocols = ipv4'
echo "Start postfix service"
systemctl enable postfix
systemctl start postfix

```

Рис. 2.17: Изменения в provisioning-скрипте mail.sh на клиенте

3 Вывод

В ходе выполнения лабораторной работы была выполнена настройка почтового сервера на базе Postfix и Dovecot, реализована доставка почты по протоколу LMTP, а также настроены механизмы SMTP-аутентификации и SMTP over TLS. Были проверены процессы приёма, передачи и доставки почтовых сообщений, проанализированы журналы работы почтовых служб и подтверждена корректность функционирования всей цепочки обработки почты. Дополнительно выполнена интеграция настроек в provisioning-скрипты Vagrant, что обеспечивает воспроизводимость конфигурации и автоматизацию развёртывания почтовой инфраструктуры. Проведённые тесты с использованием telnet, openssl и почтового клиента Evolution подтвердили корректную работу аутентификации, шифрования и доставки сообщений.

4 Контрольные вопросы

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

Пример задания формата имени пользователя для аутентификации в Dovecot с указанием домена может выглядеть следующим образом:

```
auth_username_format = %Lu@%d
```

В данном случае %Lu обозначает имя пользователя в верхнем регистре, а %d – доменную часть. Такой формат используется, когда аутентификация выполняется с учётом полного почтового адреса пользователя.

2. Какие функции выполняет почтовый Relay-сервер?

Почтовый Relay-сервер выполняет функции приёма почтовых сообщений от клиентов или других почтовых серверов и их последующей пересылки к серверу назначения. Он может осуществлять маршрутизацию почты между доменами, временное хранение сообщений при недоступности получателя, а также применять политики фильтрации, проверки и логирования почтового трафика.

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

При некорректной настройке Relay-сервера существует риск превращения его в открытый SMTP relay, который может быть использован злоумышленниками для массовой рассылки спама. Это может привести к перегрузке сервера, попаданию IP-адреса в чёрные списки, утечке информации, а также использованию сервера для распространения вредоносного программного обеспечения и фишинговых сообщений.