

Лабораторная работа №10

Расширенные настройки SMTP-сервера

Файл
Ромицына Анастасия Романовна

Содержание

1 Цель работы	6
2 Выполнение лабораторной работы	7
3 Выводы	21
4 Ответы на контрольные вопросы:	22
Список литературы	24

Список иллюстраций

2.1	Запуск в дополнительном терминале мониторинга работы почтовой службы.	7
2.2	Добавление в список протоколов, с которыми может работать Dovecot, протокола LMTP.	8
2.3	Настройка в Dovecot сервиса lmtp для связи с Postfix.	8
2.4	Переопределение в Postfix с помощью postconf передачи сообщений не на прямую, а через заданный unix-сокет.	8
2.5	Настройка в файле /etc/dovecot/conf.d/10-auth.conf формата имени пользователя для аутентификации в форме логина пользователя без указания домена.	9
2.6	Перезапуск Postfix и Dovecot.	9
2.7	Отправка из-под учётной записи своего пользователя письма с клиента.	9
2.8	Просмотр содержания логов при мониторинге почтовой службы.	10
2.9	Просмотр на сервере почтового ящика пользователя.	10
2.10	Определение в файле /etc/dovecot/conf.d/10-master.conf службы аутентификации пользователей.	11
2.11	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.	12
2.12	Временный запуск для проверки работы аутентификации SMTP-сервера (порт 25) с возможностью аутентификации.	12
2.13	Перезапуск Postfix и Dovecot.	12
2.14	Установка на клиенте telnet.	13
2.15	Получение на клиенте строки для аутентификации, подключение на клиенте к SMTP-серверу посредством telnet, тестирование соединения, проверка авторизации и завершение сессии telnet на клиенте.	14
2.16	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.	15
2.17	Замена строк в файле /etc/postfix/master.cf для того чтобы запустить SMTP-сервер на 587-м порту.	15

2.18 Настройка межсетевого экрана, разрешив работать службе smtp-submission.	16
2.19 Перезапуск Postfix.	16
2.20 Подключение на клиенте к SMTP-серверу через 587-й порт посредством openssl, тестирование подключения по telnet и проверка аутентификации.	17
2.21 Корректирование настроек почтового клиента Evolution.	18
2.22 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.	18
2.23 Внесение соответствующих изменений по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh.	19
2.24 Внесение изменения в файл /vagrant/provision/client/mail.sh.	20

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

На виртуальной машине server войдём под нашим пользователем и откроем терминал. Перейдём в режим суперпользователя. В дополнительном терминале запустим мониторинг работы почтовой службы.(рис. 2.1).



```
[arromichina@server.arromichina.net ~]$ sudo -i
[sudo] password for arromichina:
[root@server.arromichina.net ~]# tail -f /var/log/maillog
Oct 28 11:43:50 server postfix/local[15212]: 1813823434B0: to=<arromichina@arromichina.net>, relay=local, delay=0.09, delays=0.04/0.03/0/0.01, dsn=2.0.0, status=sent (delivered to maildir)
Oct 28 11:43:50 server postfix/qmgr[11438]: 1813823434B0: removed
Oct 28 11:46:29 server dovecot[11617]: pop3-login: Login: user=<arromichina>, method=PLAIN, rip=192.168.1.1, lip=192.168.1.1, mpid=15581, secured, session=<Yy40kTZCBozAqAEB>
Oct 28 11:47:31 server dovecot[11617]: pop3(arromichina)<15581><Yy40kTZCBozAqAEB>: Disconnected: Logged out top=0/0, retr=1/706, del=1/3, size=2072
Nov  5 15:03:55 server dovecot[1467]: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3, lmtp
Nov  5 15:03:56 server postfix/postfix-script[1524]: starting the Postfix mail system
Nov  5 15:03:56 server postfix/master[1541]: daemon started -- version 3.8.5, configuration /etc/postfix
Nov  5 15:24:54 server dovecot[1458]: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3, lmtp
Nov  5 15:24:55 server postfix/postfix-script[1582]: starting the Postfix mail system
Nov  5 15:24:55 server postfix/master[1596]: daemon started -- version 3.8.5, configuration /etc/postfix
```

Рис. 2.1: Запуск в дополнительном терминале мониторинга работы почтовой службы.

Добавим в список протоколов, с которыми может работать Dovecot, протокол LMTP. (рис. 2.2).

```
dovecot.conf      [-M--] 26 L:[ 10+16 26/104] *(1243/4383b) 0010 0x00[*](X)
# value inside quotes, eg.: key = "# char and trailing whitespace "
# 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 configuration
# 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
protocols = imap pop3 lmtp
```

Рис. 2.2: 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. 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.(рис. 2.3).

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

Рис. 2.3: Настройка в Dovecot сервиса lmtp для связи с Postfix.

Переопределим в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокет(рис. 2.4).

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

Рис. 2.4: Переопределение в Postfix с помощью postconf передачи сообщений не на прямую, а через заданный unix-сокет.

В файле /etc/dovecot/conf.d/10-auth.conf зададим формат имени пользователя

для аутентификации в форме логина пользователя без указания домена (рис. 2.5).

```
# 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 '@' in
# "-AT-". This translation is done after auth_username_translation changes.
auth_username_format = %Ln
```

Рис. 2.5: 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. 2.6).

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

Рис. 2.6: Перезапуск Postfix и Dovecot.

Из-под учётной записи своего пользователя отправим письмо с клиента (рис. 2.7).



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

Рис. 2.7: Отправка из-под учётной записи своего пользователя письма с клиента.

После чего посмотрим содержание логов при мониторинге почтовой службы(рис. 2.8).

The screenshot shows a terminal window with three tabs, all titled "root@server:~ - sudo -i". The content of the tabs is as follows:

```
Oct 27 12:25:30 server postfix/smtpd[20065]: disconnect from unknown[192.168.1.2] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Oct 27 12:25:30 server postfix/local[20069]: 9C89B31591: to=<anspelov@anspelov.net>, relay=local, delay=0.08, delays=0.04/0.03/0/0.01, dsn=2.0.0, status=sent (delivered to maildir)
Oct 27 12:25:30 server postfix/qmgr[15292]: 9C89B31591: removed
Oct 27 12:26:13 server dovecot[15506]: pop3-login: Login: user=<anspelov>, method=PLAIN, rip=192.168.1.1, lip=192.168.1.1, mpid=20167, secured, session=<oZxHASNCdunAqAEB>
Oct 27 12:26:35 server dovecot[15506]: pop3(anspelov)<20167><oZxHASNCdunAqAEB>: Disconnected: Logged out top=0/0, retr=1/655, del=1/2, size=1279
Oct 27 12:35:17 server dovecot[15506]: imap(anspelov)<18830><Pq7e2yJCitjAqAEC>: Disconnected: Connection closed (IDLE finished 518.291 secs ago) in=1307 out=6533 deleted=0 expunged=0 trashed=0 hdr_count=2 hdr_bytes=1265 body_count=2 body_bytes=1279
Nov 1 09:17:12 server dovecot[1347]: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3
Nov 1 09:17:15 server postfix/postfix-script[1728]: starting the Postfix mail system
Nov 1 09:17:15 server postfix/master[1740]: daemon started -- version 3.8.5, configuration /etc/postfix
Nov 1 09:26:45 server postfix/postfix-script[10187]: stopping the Postfix mail system
Nov 1 09:26:45 server postfix/master[1740]: terminating on signal 15
Nov 1 09:26:46 server postfix/postfix-script[10265]: starting the Postfix mail system
Nov 1 09:26:46 server postfix/master[10267]: daemon started -- version 3.8.5, configuration /etc/postfix
Nov 1 09:26:54 server dovecot[1347]: master: Warning: Killed with signal 15 (by pid=10289 uid=0 code=kill)
Nov 1 09:26:55 server dovecot[1493]: log(1493): Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Nov 1 09:26:56 server dovecot[10305]: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3, lmtp
```

Рис. 2.8: Просмотр содержания логов при мониторинге почтовой службы.

На сервере просмотрим почтовый ящик пользователя (рис. 2.9).

```
[root@server.arromichina.net ~]# MAIL=~/.Maildir/ mail
```

Рис. 2.9: Просмотр на сервере почтового ящика пользователя.

В файле /etc/dovecot/conf.d/10-master.conf определим службу аутентификации пользователей(рис. 2.10).

```
10-master.conf      [----] 4 L:[ 81+12 93/113 ] *(2162/2625b) 0125 0x07[*][X]
#process_limit = 1024
}

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

```

Рис. 2.10: 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 обслуживающих 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. 2.11).

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

Рис. 2.11: 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. 2.12).

```
master.cf      [-M--] 4 L:[ 1+12 13/151] *(579 /7287b) 0045 0x02[*][X]
#
# Postfix master process configuration file. For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
# -----
# service type  private unpriv  chroot  wakeup  maxproc command + args
#           (yes)   (yes)   (no)    (never) (100)
# -----
smtp  inet  n - n - - smtpd
    -o smtpd_sasl_auth_enable=yes
    -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_
#smtp    inet  n      -     n      -       1      postscreen
#smtpd   pass  -      -     n      -       -      smtpd
#dnsblog  unix  -      -     n      -       0      dnsbl_d
#tlsproxy  unix  -      -     n      -       0      tlsproxy
```

Рис. 2.12: Временный запуск для проверки работы аутентификации SMTP-сервера (порт 25) с возможностью аутентификации.

Затем перезапустим Postfix и Dovecot (рис. 2.13).

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

Рис. 2.13: Перезапуск Postfix и Dovecot.

На клиенте установим telnet(рис. 2.14).

```
[arromichina@client.arromichina.net ~]$ echo . | mail -s "LMTP test" arromichina@arromichina.net
[arromichina@client.arromichina.net ~]$ sudo -i
[sudo] password for arromichina:
[root@client.arromichina.net ~]# dnf -y install telnet
Extra Packages for Enterprise Linux 10 - x86_64 13 kB/s | 40 kB 00:02
Extra Packages for Enterprise Linux 10 - x86_64 2.5 MB/s | 4.8 MB 00:01
Rocky Linux 10 - BaseOS 862 B/s | 4.3 kB 00:05
Rocky Linux 10 - BaseOS 11 MB/s | 23 MB 00:02
Rocky Linux 10 - AppStream 15 kB/s | 4.3 kB 00:00
Rocky Linux 10 - AppStream 3.7 MB/s | 2.2 MB 00:00
Rocky Linux 10 - CRB 15 kB/s | 4.3 kB 00:00
Rocky Linux 10 - CRB 1.5 MB/s | 532 kB 00:00
Rocky Linux 10 - Extras 12 kB/s | 3.1 kB 00:00
Rocky Linux 10 - Extras 19 kB/s | 5.5 kB 00:00
Dependencies resolved.

=====
Package           Architecture Version      Repository      Size
=====
Installing:
telnet            x86_64       1:0.17-94.el10    appstream     62 k

Transaction Summary
=====
Install 1 Package

Total download size: 62 k
Installed size: 109 k
Downloading Packages:
telnet-0.17-94.el10.x86_64.rpm 1.5 MB/s | 62 kB 00:00
=====
Total          202 kB/s | 62 kB 00:00
Running transaction check
[
```

Рис. 2.14: Установка на клиенте telnet.

На клиенте получим строку для аутентификации. В качестве результата получим строку для аутентификации в формате base64. После чего подключимся на клиенте к SMTP-серверу посредством telnet: telnet server.arromichina.net 25. Теперь протестируем соединение, введя EHLO test и проверим авторизацию, задав: AUTH PLAIN. Завершим сессию telnet на клиенте (рис. 2.15).

```
250-SMTPUTF8
250 CHUNKING
EHLO test YXJyb21pY2hpbmEAYXJyb21pY2hpbmEAMTIZNDU2
250-server.arromichina.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
EHLO test YXJyb21pY2hpbmEAYXJyb21pY2hpbmEAMTIZNDU2
250-server.arromichina.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 YXJyb21pY2hpbmEAYXJyb21pY2hpbmEAMTIZNDU2
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
Connection closed by foreign host.
[arromichina@client.arromichina.net ~]$
```

Рис. 2.15: 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. 2.16).

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

Рис. 2.16: 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. 2.17).

```
master.cf      [----] 10 L:[ 19+ 1 20/156] *(1026/7337b) 0032 0x02[*][X]
#127.0.0.1:submission inet n - n - - smtpd
  submission inet n - n - - smtpd
    -o smtpd_tls_security_level=encrypt
    -o smtpd_sasl_auth_enable=yes
    -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown

#
# -o syslog_name=postfix/submission
# -o smtpd_tls_security_level=encrypt
# -o smtpd_sasl_auth_enable=yes
# -o smtpd_tls_auth_only=yes
```

Рис. 2.17: 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. 2.18).

```
r foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replicat
ion freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana g
re high-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp
ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerber
os kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-pl
ane kube-control-plane-secure kube-controller-manager kube-controller-manager
-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-work
er kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lig
htning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns
memcache minecraft minidlna mnpd mongodb mosh mountd mpd mqtt mqtt-tls ms-wb
t mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata
-dashbaord nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imagei
o ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis p
op3 pop3s postgresql privoxy prometheus-prometheus-node-exporter proxy-dhcp p
s2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis
redis-sentinel roott rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba
-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp s
mtp-submission smtps snmp snmppts snmppts-trap snmptrap spideroak-lansync spo
tify-sync squid ssdp ssh ssh-custom statsrv steam-lan-transfer steam-streamin
g stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn
syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls t
elnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn t
urns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wiregu
rd ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-dis
covery-udp wsdd wsdd-http wsman wsman xdmcp xmpp-bosh xmpp-client xmpp-local
xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper za
bbix-web-service zero-k zerotier
[root@server.arromichina.net ~]# firewall-cmd --add-service=smtp-submission
success
[root@server.arromichina.net ~]# firewall-cmd --add-service=smtp-submission -
-permanent
success
[root@server.arromichina.net ~]# firewall-cmd --reload
success
[root@server.arromichina.net ~]#
```

Рис. 2.18: Настройка межсетевого экрана, разрешив работать службе smtp-submission.

Перезапустим Postfix (рис. 2.19).

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

Рис. 2.19: Перезапуск Postfix.

На клиенте подключимся к SMTP-серверу через 587-й порт посредством openssl и протестируем подключение по telnet, проверим аутентификацию (рис. 2.20).

```
arromichina@client:~ - openssl s_client -starttls smtp -crlf -connect server.arromichina.net:587
arromichina@client:~ - openssl s_client -starttls smtp -crlf -connect server.arromichina.net:587

0020 - 7d c8 bb 11 89 d7 ef e7-37 fa 1b 62 18 f5 52 77 }.....7..b..Rw
0030 - 04 c4 12 02 06 24 ac 64-ac d7 5a 86 d0 6f 7d 43 ....$.d..Z..m.C
0040 - 72 c3 05 9c b7 8c 4f b9-6d ec a9 07 c0 92 78 9a x....0.m....x.
0050 - 05 91 68 ec 11 71 24 3f-b1 31 ed 22 44 94 1f 93 ..h..q$7.1."D...
0060 - cc d9 2a 6c 70 39 48 3e-af 46 92 12 f7 fd 7d 40 ..^pB#H.F...@]
0070 - 25 73 d9 f4 1f 64 d8 a0-f2 98 e1 81 89 b7 ec 62 %s..d.....b
0080 - 2a 47 d7 f1 09 35 ae df-a1 54 ca b1 f3 96 81 c8 *G..5..T.....
0090 - 86 50 58 1b 62 9d af 66-9e bd 64 99 2e bf 29 a5 .P.X.b..f..d..).
00a0 - b1 59 16 10 96 50 95-3b 44 c6 62 a7 94 69 1a .Y...P..;0.b..t.
00b0 - a4 d3 05 74 d8 19 6e 47-63 e0 8e 10 37 12 71 ...t..n0c....7.q
00c0 - 4f 22 4a bd 28 c1 3f ff-c9 68 d2 f0 ca 2e 40 52 07J.(?.h....@R

Start Time: 1762370202
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.arromichina.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 YXJybz21pY2hpbmEAYXJyb21pY2hpbmEMTlZNDU2
235 2.7.0 Authentication successful
```

Рис. 2.20: 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. 2.21).

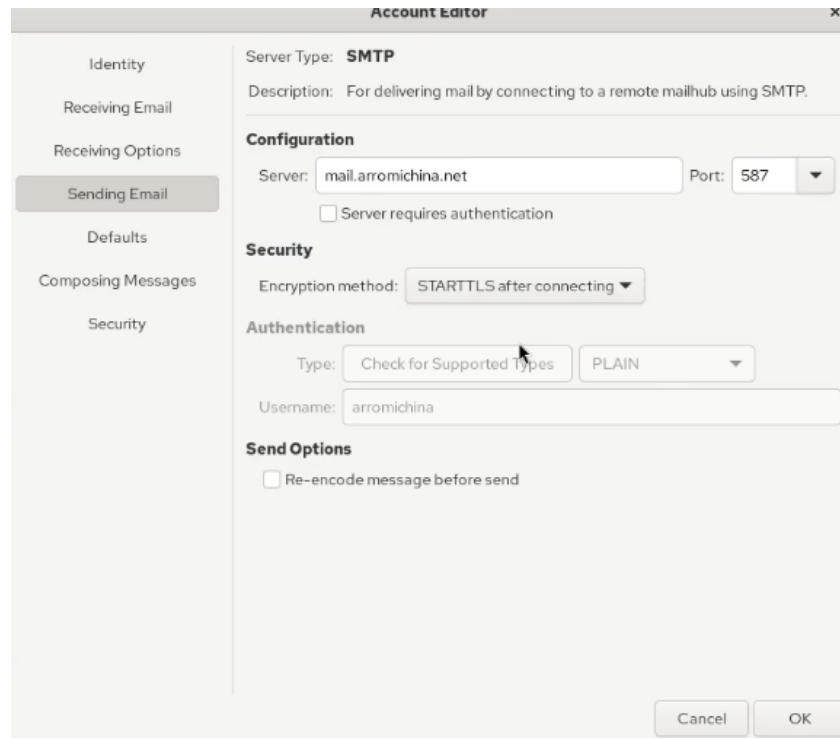


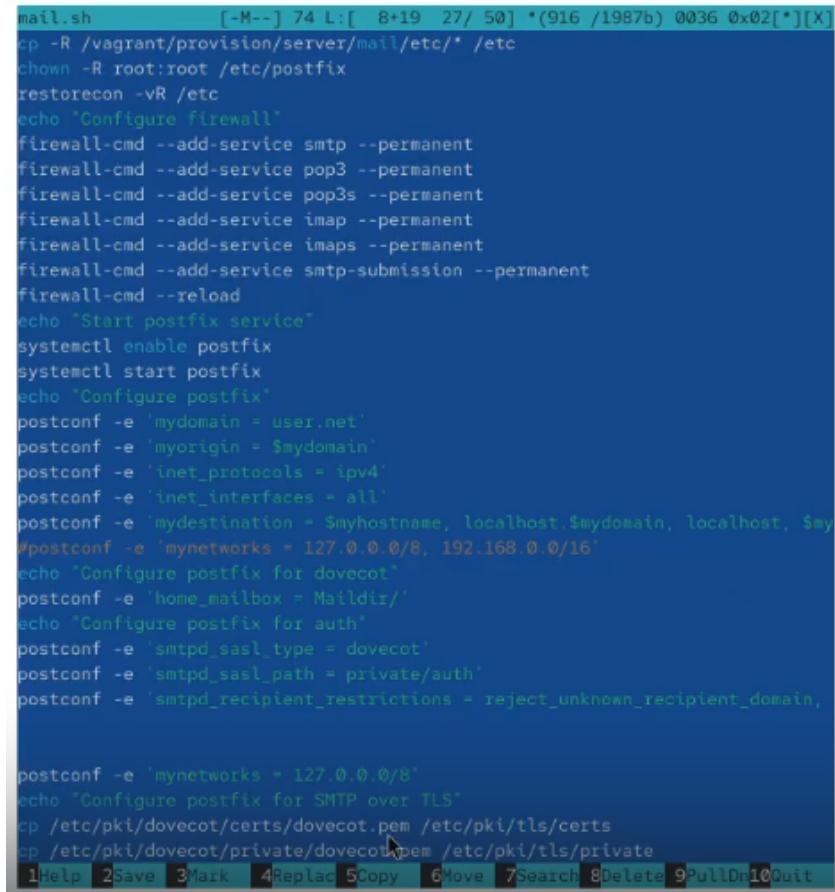
Рис. 2.21: Корректирование настроек почтового клиента Evolution.

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. 2.22).

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

Рис. 2.22: 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.

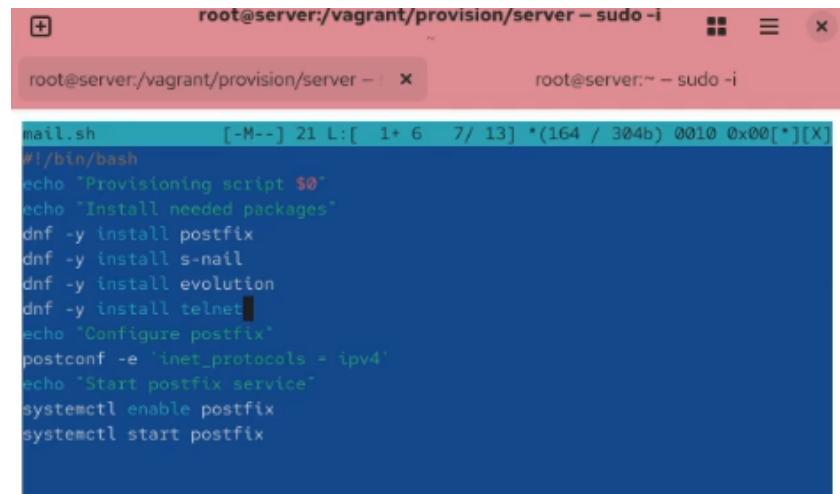
Внесём соответствующие изменения по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh (рис. 2.23).



```
mail.sh [-M--] 74 L:[ 8+19 27/ 50] *(916 /1987b) 0036 0x02[*][X]
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 = user.net'
postconf -e 'myorigin = $mydomain'
postconf -e 'inet_protocols = ipv4'
postconf -e 'inet_interfaces = all'
postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost, $my
#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,
          check_mx $myorigin, check_mx $mydomain, permit_mynetworks, permit
          defer_unauth_destination'
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
 1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDown 10Quit
```

Рис. 2.23: 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. 2.24).



The screenshot shows a terminal window with a red header bar. The title bar reads "root@server:/vagrant/provision/server - sudo -i". The main area of the terminal shows a shell script named "mail.sh" with the following content:

```
mail.sh [-M--] 21 L:[ 1+ 6 7/ 13] *(164 / 304b) 0010 0x00[*][X]
#!/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. 2.24: Внесение изменения в файл /vagrant/provision/client/mail.sh.

3 Выводы

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

4 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 пересыпает их к адресатам. Это особенно полезно, если у вас нет прямого доступа к серверу назначения или 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.

Список литературы