

Лабораторная работа №10

Расширенные настройки SMTP-сервера

Файл

Спелов Андрей Николаевич

Содержание

1 Цель работы	6
2 Выполнение лабораторной работы	7
3 Выводы	20
4 Ответы на контрольные вопросы:	21
Список литературы	23

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.	9
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.	19

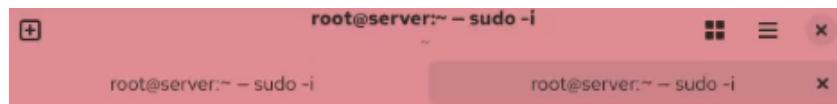
Список таблиц

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).



```
[anspelov@server anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server anspelov.net ~]# tail -f /var/log/maillog
Oct 27 12:25:30 server postfix/qmgr[15292]: 9C89B31591: from=<anspelov@anspelov.net>, size=527, nrcpt=1 (queue active)
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
```

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+15  25/103] *(1220/4360b) 0010 0x00[*][X]
# value inside quotes, eg.: key = "# char and trailing whitespace "
# Most (but not all) settings can be overridden by different protocols and/o
# 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 configu
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

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

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).

```
10-master.conf      [-M--] 5 L:[ 45+17  62/129] *(1536/3504b) 0010 0x00[*][X]
}

service submission-login {
    inet_listener submission {
        #port = 587
    }
    inet_listener submissions {
        #port = 465
    }
}

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

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

Рис. 2.6: Перезапуск Postfix и Dovecot.

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



```
anspelov@client:~  
[anspelov@client.an spelov.net ~]$ echo .| mail -s "LMTP test" an spelov@an spelov.net  
[anspelov@client.an spelov.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 anspelov.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      [-M--] 1 L:[ 81+13 94/112] *(2165/2620b) 0010 0x00[*][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 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. 2.11).

```
[root@server.anpelov.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.anpelov.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.anpelov.net ~]# postconf -e 'smtpd_recipient_restrictions = rej
ect_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, r
eject_unauth_destination, reject_unverified_recipient, permit'
[root@server.anpelov.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'
[root@server.anpelov.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--] 25 L:[ 1+22 23/150] *(1297/7318b) 0101 0x065
/
// 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).
//
// Do not forget to execute "postfix reload" after editing this file.
//
=====
// 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_recipient_domain,permit_sasl_authenticated,reject_unverified_recipient
smtpd  inet  n       -       n       -       1       postscreen
smtpd  pass  -       -       n       -       -       smtpd
dnsblog  unix  -       -       n       -       0       dnsblog
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.anpelov.net ~]# systemctl restart postfix
[root@server.anpelov.net ~]# systemctl restart dovecot
[root@server.anpelov.net ~]#
```

Рис. 2.13: Перезапуск Postfix и Dovecot.

На клиенте установим telnet(рис. 2.14).

```
[root@client.anspelov.net ~]# dnf -y install telnet
Extra Packages for Enterprise Linux 10 - x86 8.2 kB/s | 34 kB  00:04
Extra Packages for Enterprise Linux 10 - x86 2.3 MB/s | 4.8 MB  00:02
Rocky Linux 10 - BaseOS 706 B/s | 4.3 kB  00:06
Rocky Linux 10 - AppStream 379 B/s | 4.3 kB  00:11
Rocky Linux 10 - CRB 15 kB/s | 4.3 kB  00:00
Rocky Linux 10 - Extras 10 kB/s | 3.1 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 26 kB/s | 62 kB  00:02
Total 24 kB/s | 62 kB  00:02
```

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.anspelov.net 25 Теперь протестируем соединение, введя EHLO test и проверим авторизацию, задав: AUTH PLAIN Завершим сессию telnet на клиенте (рис. 2.15).

```
[root@client.an spelov.net ~]# printf 'an spelov\x00an spelov\x00123456' | base64  
4  
YW5zcGVsb3YAYW5zcGVsb3YAMTIzNDU2  
[root@client.an spelov.net ~]# telnet server.an spelov.net 25  
Trying 192.168.1.1...  
Connected to server.an spelov.net.  
Escape character is '^].  
220 server.an spelov.net ESMTP Postfix  
EHLO test  
250-server.an spelov.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 YW5zcGVsb3YAYW5zcGVsb3YAMTIzNDU2  
235 2.7.0 Authentication successful  
quit  
221 2.0.0 Bye  
Connection closed by foreign host.  
[root@client.an spelov.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.anpelov.net ~]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
[root@server.anpelov.net ~]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
[root@server.anpelov.net ~]# postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
[root@server.anpelov.net ~]# postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
[root@server.anpelov.net ~]# postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
[root@server.anpelov.net ~]# postconf -e 'smtpd_tls_security_level = may'
[root@server.anpelov.net ~]# postconf -e 'smtp_tls_security_level = may'
[root@server.anpelov.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 [-M--] 28 L:[ 7+17 24/149] *(1336/7283b) 0115 0x073 [*](X)
#
# -----
# service type  private unpriv  chroot  wakeup  maxproc command + args
#           (yes)   (yes)    (no)    (never) (100)
# -----
smtp     inet  n      -      n      -      -      smtpd
#smtp     inet  n      -      n      -      1      postscreen
#smtpd    pass  -      -      n      -      -      smtpd
#dnsblog  unix  -      -      n      -      0      dnsblog
#tlsproxy  unix  -      -      n      -      0      tlsproxy
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n      -      -      -      smtpd
submission inet n      -      n      -      -      smtpd
# -o syslog_name=postfix/submission
# -o smtpd_tls_security_level=encrypt
# -o smtpd_sasl_auth_enable=yes
# -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient
# -o smtpd_tls_auth_only=yes
# -o local_header_rewrite_clients=static:all
# -o smtpd_reject_unlisted_recipient=no
# Instead of specifying complex smtpd_<xxx>_restrictions here,
# specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
# here, and specify mua_<xxx>_restrictions in main.cf (where
# "<xxx>" is "client", "hello", "sender", "relay", or "recipient").
```

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).

```
root@server:~ - sudo -i
root@server:~ - sudo -i
root@server:~ - sudo -i

sync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy
freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galer
a ganglia-client ganglia-master git gpsd grafana gre high-availability http http
3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-
target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshel
l kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-cont
roller-manager kube-controller-manager-secure kube-nodeport-services kube-schedu
ler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ld
ap ldap libvirt libvirt-tls lightning-network llmnrr llmnrr-client llmnrr-tcp llmn
r-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh moun
td mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wa
nted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry
openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmw
ebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporte
r proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec
rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master sam
ba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp s
mtp smtp-submission smtps snmp snmp tls snmptrap spideroak-lansync s
potify-sync squid ssdp ssh ssh-custom statsrv steam-lan-transfer steam-streaming
stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn sync
thing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet t
entacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-
client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discove
ry ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd
wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix
-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-
k zerotier
[root@server.an spelov.net ~]# firewall-cmd --add-service=smtp-submission
success
[root@server.an spelov.net ~]# firewall-cmd --add-service=smtp-submission --perma
nent
success
[root@server.an spelov.net ~]# firewall-cmd --reload
success
[root@server.an spelov.net ~]#
```

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

Перезапустим Postfix (рис. 2.19).

```
[root@server.an spelov.net ~]# systemctl restart postfix
[root@server.an spelov.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).

```

TLS session ticket:
0000 - 3e 3d 13 6e 63 4f d6 c7-24 98 c7 0e 58 cc d5 c7 >=.nc0..$...X...
0010 - 61 e7 d9 2a 11 a1 86 f3-2b df a3 22 56 9a 3b cf a...*....+.."V.;.
0020 - d5 09 6f e0 64 fe c3 11-af 42 18 ba 17 ca 05 6b ..o.d....B.....k
0030 - a3 85 a0 80 52 a6 53 56-3c 53 c3 2b 95 ea d3 61 ....R.SV<S.+...a
0040 - b0 7f 32 e5 01 f9 46 6f-14 56 46 9a 34 de 94 c4 ..2...Fo.VF.4...
0050 - fc d1 75 f2 47 19 41 8f-2e 70 e2 e4 cd c7 41 b1 ..u.G.A.p....A.
0060 - f4 d9 71 56 b7 9b d5 5a-25 17 76 a8 d8 9e cf ca ..qV...Z%..v.....
0070 - e7 73 e6 de 69 8d f6 b1-f7 b8 ef ab 39 0c 68 03 .s..i.....9.h.
0080 - ac ce 81 08 8c 8e 7c 6b-0d 86 7d ca 9c 7c 10 d8 .....|k..}..|...
0090 - da de 8b 46 5b 7d 8f 36-f8 59 85 52 da 17 8c d9 ...F[...6.Y.R....
00a0 - 24 9b 22 c2 92 b4 06 2d-14 ef 67 e2 bb 16 5b ff $."....g...[.
00b0 - 93 d6 9c 54 80 58 17 07-61 ad ea d0 79 05 a4 f8 ...T.X..a...y...
00c0 - dc df 7e 6c 16 12 06 8c-36 8d 7a a3 e1 9f 0d b9 ..~l....6.z.....
Start Time: 1761990690
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.an spelov.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 YW5zcGVs b3YAYW5zcGVs b3YAMTIzNDU2
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).

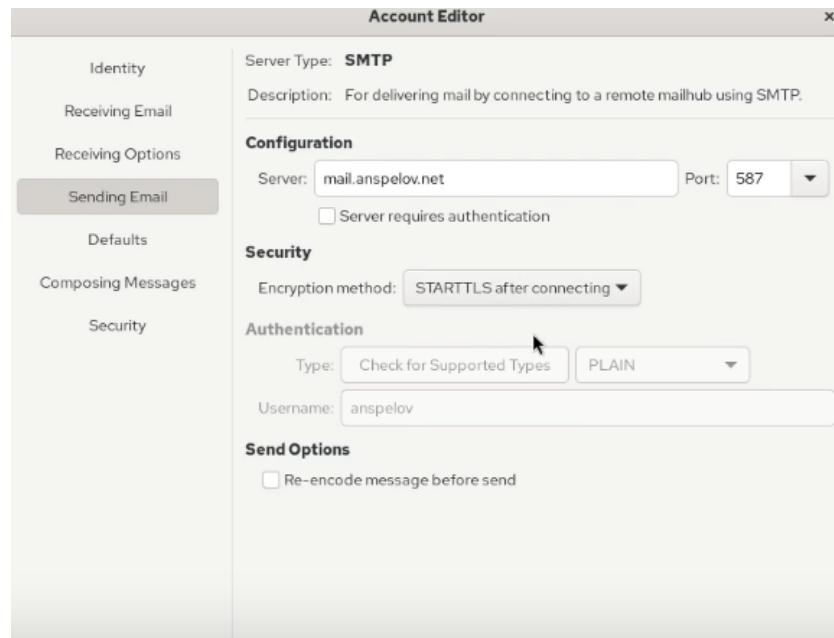


Рис. 2.21: Корректирование настроек почтового клиента Evolution.

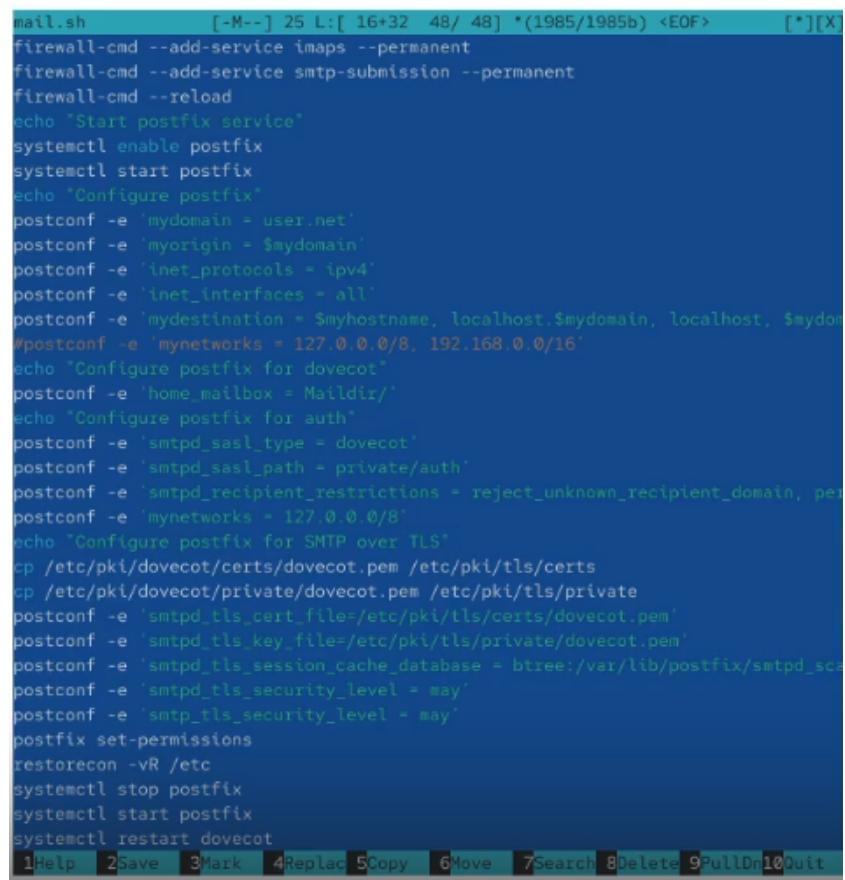
На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`. В соответствующие подкаталоги поместим конфигурационные файлы Dovecot и Postfix (рис. 2.22).

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

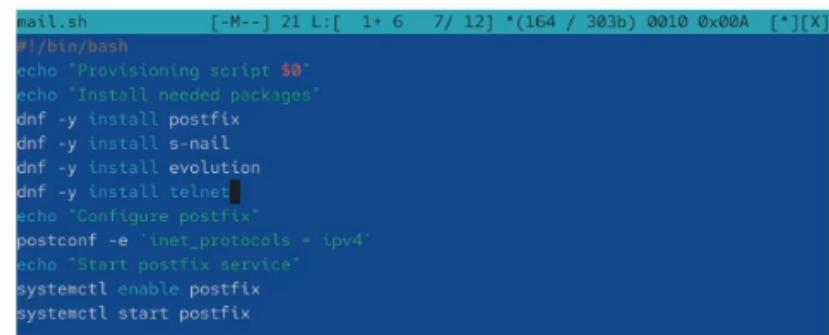
сервера в файл /vagrant/provision/server/mail.sh (рис. 2.23).



```
mail.sh      [-M--] 25 L:[ 16*32 48/ 48] *(1985/1985b) <EOF> [*][X]
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, $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'
postconf -e 'mynetworks = 127.0.0.0/8'
echo "Configure postfix for SMTP over TLS"
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_sca'
postconf -e 'smtpd_tls_security_level = may'
postconf -e 'smtp_tls_security_level = may'
postfix set-permissions
restorecon -vR /etc
systemctl stop postfix
systemctl start postfix
systemctl restart dovecot
1Help 2Save 3Mark 4Repld 5Copy 6Move 7Search 8Delete 9PullDn 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).



```
mail.sh      [-M--] 21 L:[ 1+ 6    7/ 12] *(164 / 303b) 0010 0x00A [*][X]
#!/bin/bash
echo "Provisioning script $@"
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 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.

Список литературы