

Лабораторная работа №10

Администрирование сетевых подсистем

Мишина А. А.

6 ноября 2024

Цели и задачи

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

Выполнение лабораторной работы

Настройка LMTP в Dovecote

```
# options. The paths listed here are for configure --prefix=/usr  
# --sysconfdir=/etc --localstatedir=/var  
  
# Protocols we want to be serving.  
protocols = imap pop3 lmtp  
  
# A comma separated list of IPs or hosts where to listen in for co  
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 int
```

Рис. 1: Изменение списка протоколов для работы с Dovecot

Настройка LMTP в Dovecote

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

    # Create inet listener only if you can't use the above UNIX socket
    #inet_listener lmtp {
    #    # Avoid making LMTP visible for the entire internet
    #    #address =
    #    #port =
    #}
}

service imap {
:wo|
```

Рис. 2: Настройка сервиса lmtp для связи с Postfix

Переопределим в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокет с помощью команды:

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

Настройка LMTP в Dovecote

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

# If you want to allow master users to log in by specifying the master
# username within the normal username string (ie. not using SASL mechanism's
# support for it), you can specify the separator character here. The format
# is then <username><separator><master username>. UW-INAP uses "*" as the
# separator, so that could be a good choice.
#auth_master_user_separator =

# Username to use for users logging in with ANONYMOUS SASL mechanism
#auth_anonymous_username = anonymous

# Maximum number of dovecot-auth worker processes. They're used to execute
# blocking passdb and userdb queries (eg. MySQL and PAM). They're
#:w
```

Рис. 3: Задание формата имени пользователя

Настройка LMTP в Dovecote

```
Oct 25 20:23:07 server postfix/smtpd[7698]: connect from client.aamishina.net[192.168.1.57]
Oct 25 20:23:07 server postfix/smtpd[7698]: AB372549F2: client=client.aamishina.net[192.168.1.57]
Oct 25 20:23:07 server postfix/cleanup[7702]: AB372549F2: message-id=<20241025202307.2E1701089626@client.aamishina.net>
Oct 25 20:23:07 server postfix/qmgr[7619]: AB372549F2: from=<aamishina@client.aamishina.net>, size=566, nrcpt=1 (queue active)
Oct 25 20:23:07 server postfix/smtpd[7698]: disconnect from client.aamishina.net[192.168.1.57] ehlo=2 starttls=1 mail=1 rcpt=1
data=1 quit=1 commands=7
Oct 25 20:23:07 server dovecot[7665]: lmtp(7705): Connect from local
Oct 25 20:23:07 server dovecot[7665]: lmtp(aamishina)<7705><BtlfMSv+G2cZHgAA56Wmmg>: msgid=<20241025202307.2E1701089626@client
.aamishina.net>; saved mail to INBOX
Oct 25 20:23:07 server dovecot[7665]: lmtp(7705): Disconnect from local: Logged out (state=READY)
Oct 25 20:23:07 server postfix/lmtp[7704]: AB372549F2: to=<aamishina@server.aamishina.net>, relay=server.aamishina.net[private
/dovecot-lmtp], delay=0.28, delays=0.04/0.03/0.09/0.13, dsn=2.0.0, status=sent (250 2.0.0 <aamishina@server.aamishina.net> Btl
fMSv+G2cZHgAA56Wmmg Saved)
Oct 25 20:23:07 server postfix/qmgr[7619]: AB372549F2: removed
```

Рис. 4: Просмотр мониторинга почтовой службы

Настройка LMTP в Dovecote

```
[aamishina@server.aamishina.net ~]$ MAIL=~/.Maildir/ mail  
s-nail version v14.9.22. Type '?' for help  
/home/aamishina/Maildir: 2 messages 1 new  
  1 aamishina          2024-10-25 18:02   18/640  
•N 2 aamishina@client.aam 2024-10-25 20:23   21/864  "LMTP test  
& |
```

Рис. 5: Просмотр почтового ящика пользователя

Настройка SMTP-аутентификации

```
# To give the caller full permissions to lookup all users, set the mode
# something else than 0666 and Dovecot lets the kernel enforce the
# permissions (e.g. 0777 allows everyone full permissions).
unix_listener /var/spool/postfix/private/auth {
    group = postfix
    user = postfix
    mode = 0660
}
unix_listener auth-userdb {
    mode = 0666
    user = dovecot
    #group =
}

# Postfix smtp-auth
#unix_listener /var/spool/postfix/private/auth {
#    mode = 0666
#}
```

:|

Рис. 6: Определение службы аутентификации пользователей

Настройка SMTP-аутентификации

```
[root@server.aamishina.net ~]# vim /etc/dovecot/conf.d/10-master.conf
[root@server.aamishina.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.aamishina.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.aamishina.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.aamishina.net ~]# postconf -e 'mynetworks = 127.0.0.0/8
> ^C
[root@server.aamishina.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'
[root@server.aamishina.net ~]#
```

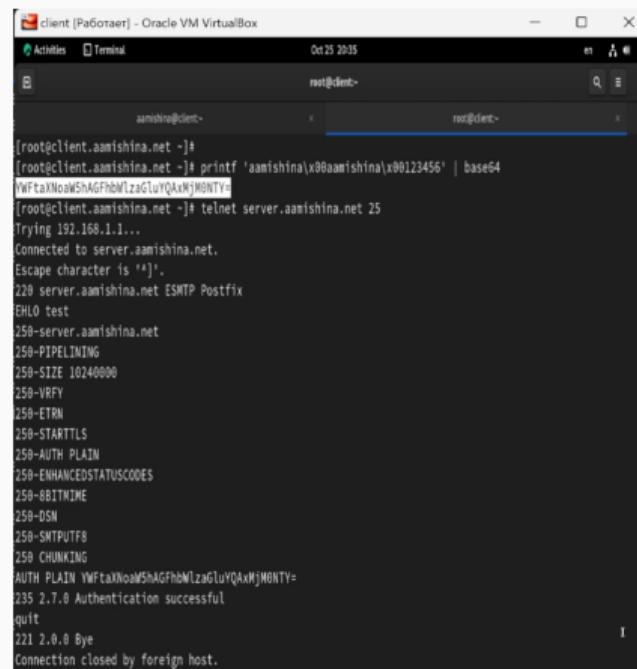
Рис. 7: Конфигурации Postfix

Настройка SMTP-аутентификации

```
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
#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
#submission inet n      -      n      -      -      smtpd
#      -o syslog_name=postfix/submission
#      -o smtpd_tls_security_level=encrypt
#      -o smtpd_sasl_auth_enable=yes
#      -o smtpd_tls_auth_only=yes
#      -o smtpd_reject_unlisted_recipient=no
#      -o smtpd_client_restrictions=$mua_client_restrictions
:w|
```

Рис. 8: Временный запуск SMTP-сервера

Настройка SMTP-аутентификации



The screenshot shows a terminal window titled "client [Работает] - Oracle VM VirtualBox". The window has two tabs: "root@client-" and "root@client-". The "root@client-" tab is active, displaying a telnet session to an SMTP server. The session starts with a command to print a base64 encoded string, followed by a connection to the server, an EHLO test, and a series of 250 responses for various service extensions. It then performs an AUTH PLAIN command with the same base64 string, receives a 235 response indicating successful authentication, and finally quits the session.

```
[root@client.aamishina.net ~]# [root@client.aamishina.net ~]# printf 'aamishina\x00aamishina\x00123456' | base64 [root@client.aamishina.net ~]# [root@client.aamishina.net ~]# telnet server.aamishina.net 25  
Trying 192.168.1.1...  
Connected to server.aamishina.net.  
Escape character is ']'.  
220 server.aamishina.net ESMTP Postfix  
EHLO test  
250-server.aamishina.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 YWFtaXNoaWShAGFhbWlzaGlwYQAxMjM0NTY=  
235 2.7.8 Authentication successful  
quit  
221 2.0.0 Bye  
Connection closed by foreign host.
```

Рис. 9: Получение строки для аутентификация и проверка посредством telnet

Настройка SMTP over TLS

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

Рис. 10: Конфигурации Postfix для настройки TLS

Настройка SMTP over TLS

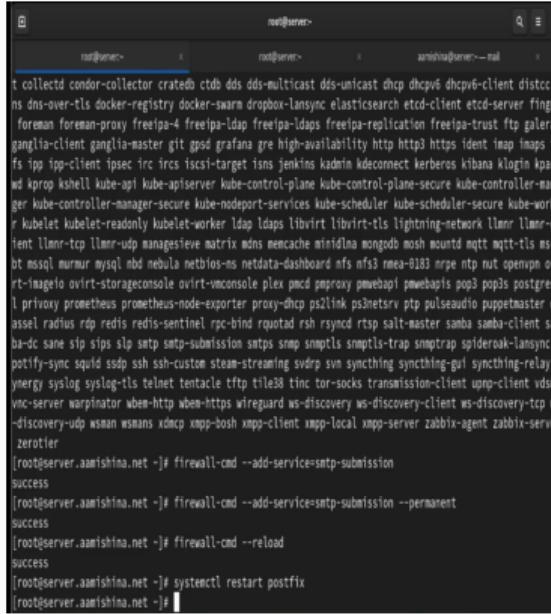
```
#smtp inet n - n - - smtpd -o smtpd_sasl_auth_enable=yes -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
smtp    inet  n      -      n      -      -      smtpd
#smtp    inet  n      -      n      -      1      postscreen
#smtpd   pass  -      -      n      -      -      smtpd
#dnsblog  unix  -      -      n      -      0      dnsblog
#tlsproxy  unix  -      -      n      -      0      tlsproxy
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_recipient_domain,permit_sasl_authenticated,reject
#submission inet n      -      n      -      -      smtpd
#  -o syslog_name=postfix/submission
#  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_tls_auth_only=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
```

20,32

2%

Рис. 11: Изменение конфигураций для запуска SMTP-сервера на 587-порту

Настройка SMTP over TLS

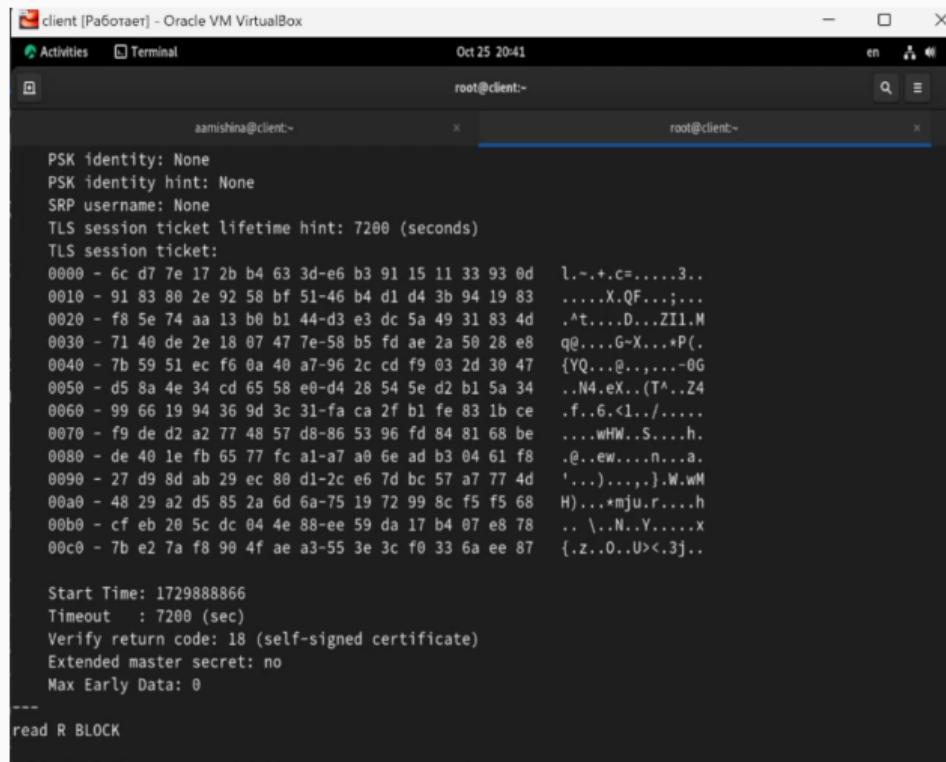


The screenshot shows a terminal window titled 'root@server~' with three tabs open: 'root@server~', 'root@server~', and 'root@server~ -- mail'. The terminal displays a long list of service names, likely from a package manager or a system configuration tool. Below this list, several commands are entered and executed:

```
[root@server ~]# firewall-cmd --add-service=smtp-submission
success
[root@server ~]# firewall-cmd --add-service=smtp-submission --permanent
success
[root@server ~]# firewall-cmd --reload
success
[root@server ~]# systemctl restart postfix
[root@server ~]#
```

Рис. 12: Настройка межсетевого экрана для работы службы smtp-submission

Настройка SMTP over TLS



```
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - 6c d7 7e 17 2b b4 63 3d-e6 b3 91 15 11 33 93 0d l..+.c=....3..
0010 - 91 83 80 2e 92 58 bf 51-46 b4 d1 d4 3b 94 19 83 .....X.QF....;...
0020 - f8 5e 74 aa 13 b0 b1 44-d3 e3 dc 5a 49 31 83 4d .^t....D....ZI1.M
0030 - 71 40 de 2e 18 07 47 7e-58 b5 fd ae 2a 50 28 e8 q@....G-X....P(. 
0040 - 7b 59 51 ec f6 0a 40 a7-96 2c cd f9 03 2d 30 47 {YQ....@,...,-0G
0050 - d5 8a 4e 34 cd 65 58 e0-d4 28 54 5e d2 b1 5a 34 ..N4.eX..(T^.Z4
0060 - 99 66 19 94 36 9d 3c 31-fa ca 2f b1 fe 83 1b ce .f..6.<1.../.....
0070 - f9 de d2 a2 77 48 57 d8-86 53 96 fd 84 81 68 be ....WHW..S....h.
0080 - de 40 1e fb 65 77 fc a1-a7 a0 6e ad b3 04 61 f8 @..ew....n...a.
0090 - 27 d9 8d ab 29 ec 80 d1-2c e6 7d bc 57 a7 77 4d '...).,...,)..W.wM
00a0 - 48 29 a2 d5 85 2a 6d 6a-75 19 72 99 8c f5 f5 68 H)...*mju.r....h
00b0 - cf eb 20 5c dc 04 4e 88-ee 59 da 17 b4 07 e8 78 ... \...N..Y....x
00c0 - 7b e2 7a f8 90 4f ae a3-55 3e 3c f0 33 6a ee 87 {.z..0..U><.3j.. 

Start Time: 1729888866
Timeout   : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
```

Рис. 13: Подключение через openssl к SMTP-серверу

Настройка SMTP over TLS

Рис. 14: Проверка подключения и аутентификации по telnet

Настройка SMTP over TLS

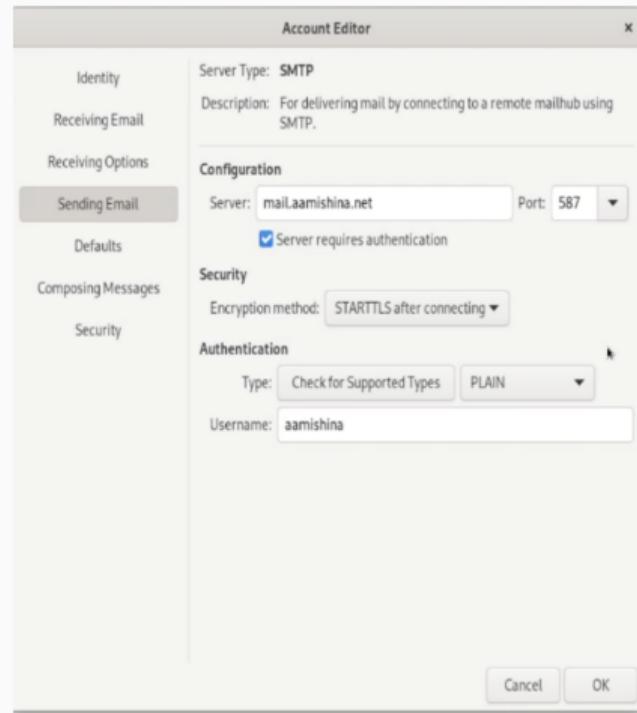


Рис. 15: Изменение настроек учетной записи Evolution

Настройка SMTP over TLS

```
[aamishina@server.aamishina.net ~]$ MAIL=-/Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/aamishina/Maildir: 3 messages 1 unread
  1 aamishina      2024-10-25 18:02  18/640
•U 2 aamishina@client.aam 2024-10-25 20:23  21/864  "LMTTP test"
  3 aamishina      2024-10-25 20:47  22/818
& 3
[-- Message 3 -- 22 lines, 818 bytes --]:
Message-ID: <55dfc8eb023879cfdb4092e62453e229e72a5041.camel@aamishina.net>
Subject:
From: aamishina <aamishina@aamishina.net>
To: aamishina@aamishina.net
Date: Fri, 25 Oct 2024 20:47:18 +0000
  □

SMTP over TLS
&
```

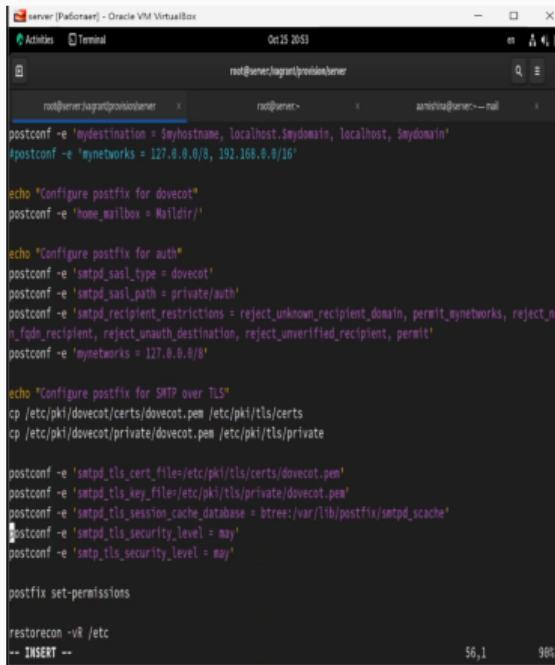
Рис. 16: Проверка корректности отправки почтовых сообщений с помощью Evolution

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
[root@server.aamishina.net ~]# cd /vagrant/provision/server
[root@server.aamishina.net server]# cp -R /etc/dovecot/dovecot.conf /vagrant/provision/server/mail/etc/do
vecot/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/dovecot.conf'? y
[root@server.aamishina.net server]# cp -R /etc/dovecot/conf.d/10-master.conf /vagrant/provision/server/ma
il/etc/dovecot/conf.d/
[root@server.aamishina.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.aamishina.net server]# mkdir -p /vagrant/provision/server/mail/etc/postfix/
[root@server.aamishina.net server]# cp -R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postf
ix/
[root@server.aamishina.net server]# vim /vagrant/provision/server/mail.sh
```

Рис. 17: Создание окружения для внесения изменений в настройки окружающей среды

Внесение изменений в настройки внутреннего окружения виртуальной машины



The screenshot shows a terminal window titled "server [Fedorov] - Oracle VM VirtualBox". It displays a shell session with the root user. The terminal has three tabs open: "root@server:/vagrant/provision/server", "root@server:~" (the current tab), and "admin@server:~-- mail". The content of the current tab shows a shell script named "mail.sh" with the following code:

```
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, reject_no_n_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, 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_scache'
postconf -e 'smtpd_tls_security_level = may'
postconf -e 'smtp_tls_security_level = may'

postfix set-permissions

restorecon -vR /etc
-- INSERT --
```

The status bar at the bottom of the terminal window indicates "56,1" and "98%".

Рис. 18: Изменение файла /vagrant/provision/server/mail.sh

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
aamishina@client:~>
#!/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. 19: Изменение файла /vagrant/provision/client/mail.sh

Заключение

Выводы

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