

Лабораторная работа №10

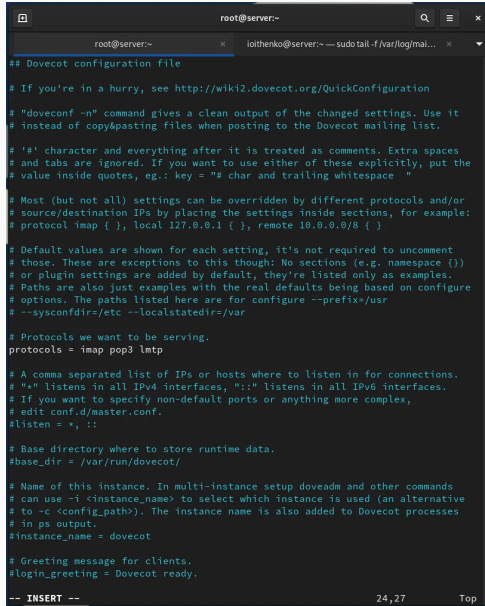
Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Российский университет дружбы народов, Москва, Россия

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

Выполнение лабораторной работы



```
## Dovecot configuration file

# If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration

# "doveconf -n" command gives a clean output of the changed settings. Use it
# instead of copy&pasting files when posting to the Dovecot mailing list.

# '#' character and everything after it is treated as comments. Extra spaces
# and tabs are ignored. If you want to use either of these explicitly, put the
# 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 configure
# 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 connections.
# "*" listens in all IPv4 interfaces, ":::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
#listen = *, ::


# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Name of this instance. In multi-instance setup doveadm and other commands
# can use -i <instance_name> to select which instance is used (an alternative
# to -c <config_path>). The instance name is also added to Dovecot processes
# in ps output.
#instance_name = dovecot

# Greeting message for clients.
#login_greeting = Dovecot ready.

-- INSERT --
```

Рис. 1: Изменение списка протоколов для работы с Dovecot

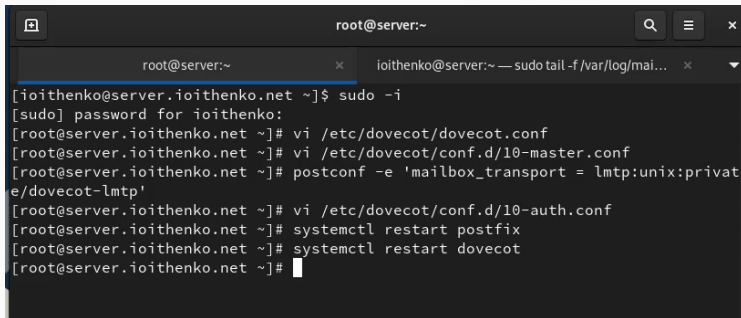


```
root@server:~  
#ssl = yes  
}  
}  
  
service submission-login {  
    inet_listener submission {  
        #port = 587  
    }  
}  
  
service lmtpl {  
    unix_listener /var/spool/postfix/private/dovecot-lmtpl {  
        group = postfix  
        user = postfix  
        mode = 0600  
    }  
}  
  
service imap {  
    # Most of the memory goes to mmap()ing files. You may need to increase this  
    # limit if you have huge mailboxes.  
    #vsz_limit = $default_vsz_limit  
  
    # Max. number of IMAP processes (connections)  
    #process_limit = 1024  
}  
  
service pop3 {  
    # Max. number of POP3 processes (connections)  
    #process_limit = 1024  
}  
  
service submission {  
    # Max. number of SMTP Submission processes (connections)  
    #process_limit = 1024  
}  
  
service auth {  
    # auth_socket_path points to this userdb socket by default. It's typically  
    # used by dovecot-lda, doveadm, possibly imap process, etc. Users that have  
    # full permissions to this socket are able to get a list of all usernames and  
    # get the results of everyone's userdb lookups.  
:  
wq
```

Рис. 2: Настройка сервиса lmtpl для связи с Postfix

```
root@server:~  
# Time to live for cached data. After TTL expires the cached record is no  
# longer used, *except* if the main database lookup returns internal failure.  
# We also try to handle password changes automatically: If user's previous  
# authentication was successful, but this one wasn't, the cache isn't used.  
# For now this works only with plaintext authentication.  
#auth_cache_ttl = 1 hour  
# TTL for negative hits (user not found, password mismatch).  
# 0 disables caching them completely.  
#auth_cache_negative_ttl = 1 hour  
  
# Space separated list of realms for SASL authentication mechanisms that need  
# them. You can leave it empty if you don't want to support multiple realms.  
# Many clients simply use the first one listed here, so keep the default realm  
# first.  
#auth_realms =  
  
# Default realm/domain to use if none was specified. This is used for both  
# SASL realms and appending @domain to username in plaintext logins.  
#auth_default_realm =  
  
# List of allowed characters in username. If the user-given username contains  
# a character not listed in here, the login automatically fails. This is just  
# an extra check to make sure user can't exploit any potential quote escaping  
# vulnerabilities with SQL/LDAP databases. If you want to allow all characters,  
# set this value to empty.  
#auth_username_chars = abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234  
567890.-_@  
  
# Username character translations before it's looked up from databases. The  
# value contains series of from -> to characters. For example "#@/@" means  
# that '#' and '/' characters are translated to '@'.  
#auth_username_translation =  
  
# 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-IMAP uses "*" as the  
-- INSERT --  
51,27 16%
```

Рис. 3: Задание формата имени пользователя



The image shows a terminal window with a dark background. At the top, there is a title bar with the text 'root@server:~' and some icons. Below the title bar, there are two tabs: 'root@server:~' and 'ioithenko@server:~ — sudo tail -f /var/log/mai...'. The main content of the terminal is a series of commands and their outputs. The user 'ioithenko' runs 'sudo -i' to become root. Then, root runs 'vi /etc/dovecot/dovecot.conf', 'vi /etc/dovecot/conf.d/10-master.conf', and 'postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp''. After that, root runs 'vi /etc/dovecot/conf.d/10-auth.conf', 'systemctl restart postfix', and 'systemctl restart dovecot'. The terminal ends with a prompt for root at the server.

```
root@server:~  
[ioithenko@server.ioithenko.net ~]$ sudo -i  
[sudo] password for ioithenko:  
[root@server.ioithenko.net ~]# vi /etc/dovecot/dovecot.conf  
[root@server.ioithenko.net ~]# vi /etc/dovecot/conf.d/10-master.conf  
[root@server.ioithenko.net ~]# postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'  
[root@server.ioithenko.net ~]# vi /etc/dovecot/conf.d/10-auth.conf  
[root@server.ioithenko.net ~]# systemctl restart postfix  
[root@server.ioithenko.net ~]# systemctl restart dovecot  
[root@server.ioithenko.net ~]#
```

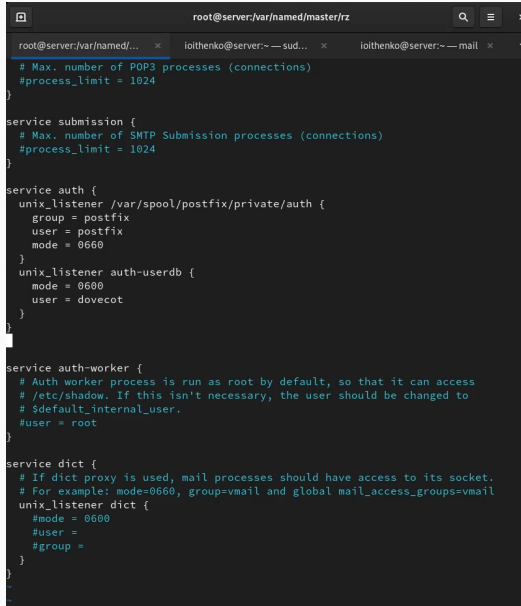
Рис. 4: Перезапуск служб

```
Nov  1 17:11:46 server postfix/postfix-script[7468]: starting the Postfix mail system
Nov  1 17:11:46 server postfix/master[7470]: daemon started -- version 3.5.9, configuration /etc/postfix
Nov  1 17:38:06 server postfix/smtpd[7521]: connect from client.ioithenko.net[192.168.1.30]
Nov  1 17:38:06 server postfix/smtpd[7521]: 6134E14EB4: client=client.ioithenko.net[192.168.1.30]
Nov  1 17:38:06 server postfix/cleanup[7525]: 6134E14EB4: message-id=<20241101173805.DC89810A99DF@client.ioithenko.net>
Nov  1 17:38:06 server postfix/smtpd[7521]: disconnect from client.ioithenko.net[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Nov  1 17:38:06 server postfix/qmgr[7472]: 6134E14EB4: from=<ioithenko@client.ioithenko.net>, size=566, nrcpt=1 (queue active)
Nov  1 17:38:06 server dovecot[7178]: lmtp(7528): Connect from local
Nov  1 17:38:06 server dovecot[7178]: lmtp(ioithenko)<7528><JiFmIP4RJWdoHQAATuTp8Q>: msgid=<20241101173805.DC89810A99DF@client.ioithenko.net>: saved mail to INBOX
Nov  1 17:38:06 server postfix/lmtp[7527]: 6134E14EB4: to=<ioithenko@server.ioithenko.net>, relay=server.ioithenko.net[private/dovecot-lmtp], delay=0.26, delays=0.03/0.02/0.12/0.09, dsn=2.0.0, status=sent (250 2.0.0 <ioithenko@server.ioithenko.net> JiFmIP4RJWdoHQAATuTp8Q Saved)
Nov  1 17:38:06 server postfix/qmgr[7472]: 6134E14EB4: removed
Nov  1 17:38:06 server dovecot[7178]: lmtp(7528): Disconnect from local: Logged out (state=READY)
```

Рис. 5: Просмотр мониторинга почтовой службы


```
s have version v14.9.22: type ? for help
/home/ioithenko/Maildir: 4 messages 1 new 3 unread
  1 ioithenko      2024-10-30 15:03   18/641   "test1       "
U  2 ioithenko      2024-10-30 15:04   18/642   "test2       "
U  3 ioithenko      2024-10-30 15:11   18/642   "test1       "
•N 4 ioithenko@client.ioi 2024-11-01 17:38   21/864   "LMTP test   "
&
```

Рис. 6: Просмотр почтового ящика пользователя

A terminal window with a dark background and light-colored text. The title bar shows the path 'root@server:/var/named/master/rz'. The terminal has three tabs: 'root@server:/var/named/...', 'ioithenko@server:~ — sud...', and 'ioithenko@server:~ — mail'. The active tab is the first one. The content of the terminal is a Postfix configuration file snippet. It defines services for POP3, SMTP submission, authentication (auth), and an authentication worker (auth-worker). The 'auth' service has two listeners: one for the main authentication socket and another for the 'auth-userdb' database. The 'auth-worker' service is configured to run as root. The 'dict' service is also configured with a listener. The configuration uses standard Postfix syntax with 'service' blocks and 'unix_listener' directives.

```
root@server:/var/named/master/rz
# Max. number of POP3 processes (connections)
#process_limit = 1024
}

service submission {
    # Max. number of SMTP Submission processes (connections)
    #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
    }
}

service auth-worker {
    # Auth worker process is run as root by default, so that it can access
    # /etc/shadow. If this isn't necessary, the user should be changed to
    # $default_internal_user.
    #user = root
}

service dict {
    # If dict proxy is used, mail processes should have access to its socket.
    # For example: mode=0660, group=vmmail and global mail_access_groups=vmmail
    unix_listener dict {
        #mode = 0600
        #user =
        #group =
    }
}
```

Рис. 7: Определение службы аутентификации пользователей

```
[root@server.ioithenko.net rz]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.ioithenko.net rz]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.ioithenko.net rz]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'
[root@server.ioithenko.net rz]# postconf -e 'mynetworks = 127.0.0.0/8'
[root@server.ioithenko.net rz]#
```

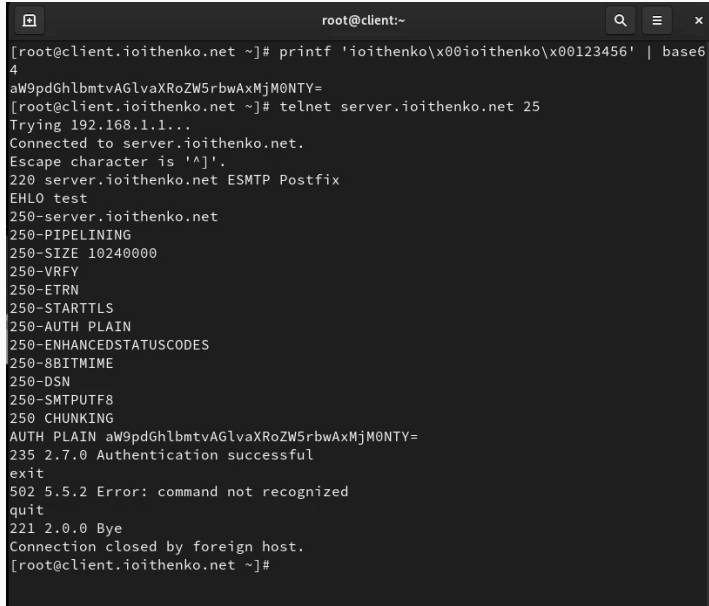
Рис. 8: Конфигурации Postfix

```
root@server:~  
#  
# 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_restr  
ictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticat  
ed,reject  
#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  
"/etc/postfix/master.cf" 133L, 6489B 12,127 Top
```

Рис. 9: Временный запуск SMTP-сервера

```
[root@server.ioithenko.net ~]# vi /etc/postfix/master.cf  
[root@server.ioithenko.net ~]# systemctl restart postfix  
[root@server.ioithenko.net ~]# systemctl restart dovecot
```

Рис. 10: Перезапуск служб

A terminal window titled 'root@client:~' with search, menu, and close buttons. It shows a telnet session to 'server.ioithenko.net' on port 25. The user enters a base64-encoded string for authentication, which is accepted. Then, they enter an unrecognized command, resulting in an error message, and finally type 'quit' to end the session.

```
root@client:~  
[root@client.ioithenko.net ~]# printf 'ioithenko\x00ioithenko\x00123456' | base64  
aW9pdGhlbmtvAGlvaXRoZW5rbwAxMjM0NTY=  
[root@client.ioithenko.net ~]# telnet server.ioithenko.net 25  
Trying 192.168.1.1...  
Connected to server.ioithenko.net.  
Escape character is '^]'.  
220 server.ioithenko.net ESMTP Postfix  
EHLO test  
250-server.ioithenko.net  
250-PIPELINING  
250-SIZE 10240000  
250-VERFY  
250-ETRN  
250-STARTTLS  
250-AUTH PLAIN  
250-ENHANCEDSTATUSCODES  
250-8BITMIME  
250-DSN  
250-SMTPUTF8  
250 CHUNKING  
AUTH PLAIN aW9pdGhlbmtvAGlvaXRoZW5rbwAxMjM0NTY=  
235 2.7.0 Authentication successful  
exit  
502 5.5.2 Error: command not recognized  
quit  
221 2.0.0 Bye  
Connection closed by foreign host.  
[root@client.ioithenko.net ~]#
```

Рис. 11: Получение строки для аутентификация и проверка посредством telnet

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

Рис. 12: Конфигарции Postfix для настройки TLS

```
root@server:~  
#  
# 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  
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  
#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=$mua_client_restrictions  
# -o smtpd_helo_restrictions=$mua_helo_restrictions  
# -o smtpd_sender_restrictions=$mua_sender_restrictions  
# -o smtpd_recipient_restrictions=  
# -o smtpd_relay_restrictions=permit_sasl_authenticated,reject  
# -o milter_macro_daemon_name=ORIGINATING  
#smtps inet n - n - - smtpd  
# -o syslog_name=postfix/smtps  
# -o smtpd_tls_wrappermode=yes  
# -o smtpd_sasl_auth_enable=yes  
# -o smtpd_reject_unlisted_recipient=no  
# -o smtpd_client_restrictions=$mua_client_restrictions  
# -o smtpd_helo_restrictions=$mua_helo_restrictions
```

13,32

Top

Рис. 13: Изменение конфигураций для запуска SMTP-сервера на 587-порту


```
[root@server.ioithenko.net ~]# firewall-cmd --add-service=smtp-submission
success
[root@server.ioithenko.net ~]# firewall-cmd --add-service=smtp-submission --perm
anent
success
[root@server.ioithenko.net ~]# firewall-cmd --reload
success
[root@server.ioithenko.net ~]# systemctl restart postfix
[root@server.ioithenko.net ~]#
```

Рис. 14: Настройка межсетевого экрана для работы службы smtp-submission

```

root@client:~
Resumption PSK: 4FBE4A1C1B15523FB858C099E4002AD65B334468F5CE997FDBDCDA38623A
10443B651200E7E71A4DA7A3D8C2265FAEFC
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - 77 49 1b b8 1f 95 5e 14-38 6a 6f d1 52 3b 79 50 wI....^..8jo.R;yp
0010 - ee e4 be 82 df ac 1c c1-5c 39 43 cc 73 31 49 a2 ..... \0C.sI.
0020 - 8e 17 cc d5 87 b7 95 8f-cd 94 ca 8f cd 0d 17 bd .....
0030 - c3 58 08 7b d8 0b b2 6f-5a 0f 6d 56 e6 bb 17 4d .X.{...oZ.mV...M
0040 - d8 5d ff 08 ac 48 07 39-ef 21 69 4d fc e4 4f 2d .]...H.9.!iM..0-
0050 - 0a 4b 50 fe e3 39 e2 0c-32 26 63 cb 01 f9 79 aa .KP..9..2&c...y.
0060 - ea 2b dc 0e 3d 09 b0 97-07 ae f6 19 ca 6a de 48 .+..=.....j.H
0070 - c4 62 d4 54 93 a5 9a 0e-53 37 8d d3 d8 05 58 59 .b.T...S7...XY
0080 - 51 7a 9f 26 0c bc 6b 13-39 f6 fa 57 71 26 21 a7 Qz.&...k.9..Wq&!
0090 - dd 3e c8 75 c6 bc 00 85-87 e2 fc 88 34 f9 16 e5 .>.u.....4...
00a0 - 83 0a 06 dd 26 01 f1 cb-2d 3a 67 23 2d 65 98 1f ....&...-:g#-e..
00b0 - 1a dd bc 60 7c b6 84 84-fc 0d c0 8b d0 be 28 3b ...]|.....(;
00c0 - e9 09 42 01 ec 9c 03 16-86 98 3d 6c 1d fd 9a 97 ..B.....=l....

Start Time: 1730489714
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.ioithenko.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 aW9pdGh1bmtvAGlvaXRozW5rbwAxMjM0NTY=
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
closed
[root@client.ioithenko.net ~]#

```

Рис. 15: Проверка подключения и аутентификации по openssl

Account Editor x

Identity
Receiving Email
Receiving Options
Sending Email
Defaults
Composing Messages
Security

Server Type: **SMTP**
Description: For delivering mail by connecting to a remote mailhub using SMTP.

Configuration

Server: Port: ▼

☒ Server requires authentication

Security

Encryption method: ▼

Authentication

Type: ▼

Username:

Cancel OK

Рис. 16: Изменение настроек учетной записи Evolution

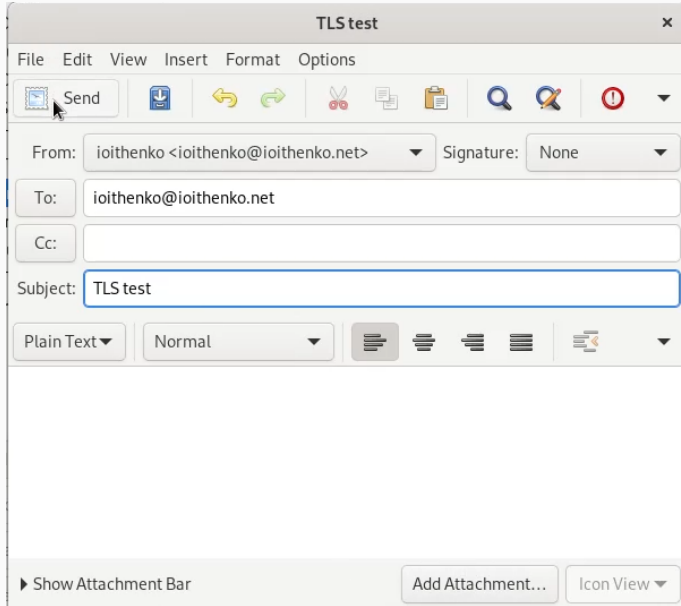


Рис. 17: Отправка письма с Evolution

```
[ioithenko@server.ioithenko.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.22.  Type '?' for help
/home/ioithenko/Maildir: 5 messages 4 unread
  1 ioithenko          2024-10-30 15:03   18/641   "test1           "
•U 2 ioithenko          2024-10-30 15:04   18/642   "test2           "
  U 3 ioithenko          2024-10-30 15:11   18/642   "test1           "
  U 4 ioithenko@client.ioi 2024-11-01 17:38   21/864   "LMTP test       "
  U 5 ioithenko          2024-11-01 19:39   22/813   "TLS test        "
& 5
[-- Message 5 -- 22 lines, 813 bytes --]:
Message-ID: <e85b17469ef4654f50af8ca747942e55930b7019.camel@ioithenko.net>
Subject: TLS test
From: ioithenko <ioithenko@ioithenko.net>
To: ioithenko@ioithenko.net
Date: Fri, 01 Nov 2024 19:39:25 +0000
```

Рис. 18: Проверка корректности отправки почтовых сообщений с помощью Evolution

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

Рис. 19: Создание окружения для внесения изменений в настройки окружающей среды

Выводы

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