

Лабораторная работа 10

Ярметов Камран

17 февраля, 2023., Москва, Россия

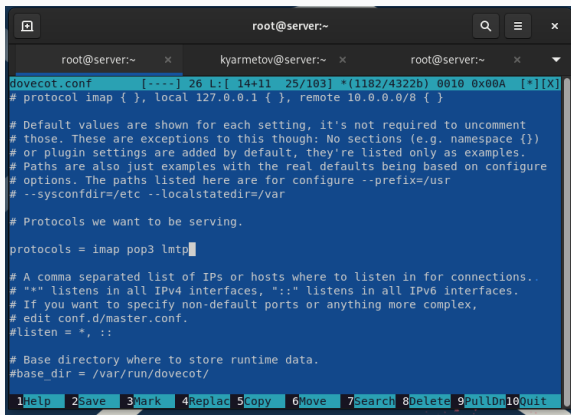
Российский Университет Дружбы Народов

Цель лабораторной работы

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

Выполнение лабораторной работы

Настройка LMTP в Dovecot



```
root@server:~
dovecot.conf [----] 26 L: [ 14+11 25/103] *(1182/4322b) 0010 0x00A [*][X]
# 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

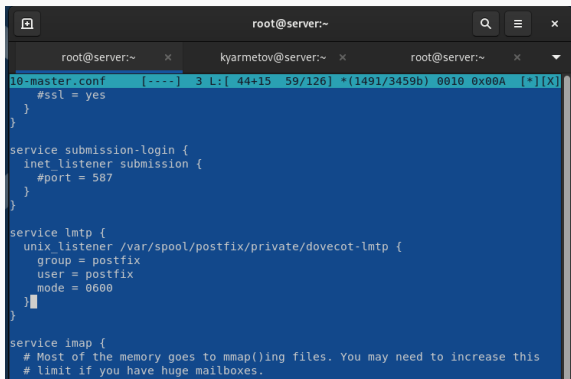
# A comma separated list of IPs or hosts where to listen in for connections..
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
#listen = *, ::

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

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullOn10Quit
```

Figure 1: файл dovecot.conf

Настройка LMTP в Dovecot



```
root@server:~
10-master.conf [----] 3 L: [ 44+15 59/126] *(1491/3459b) 0010 0x00A [*][X]
#ssl = yes
}
}

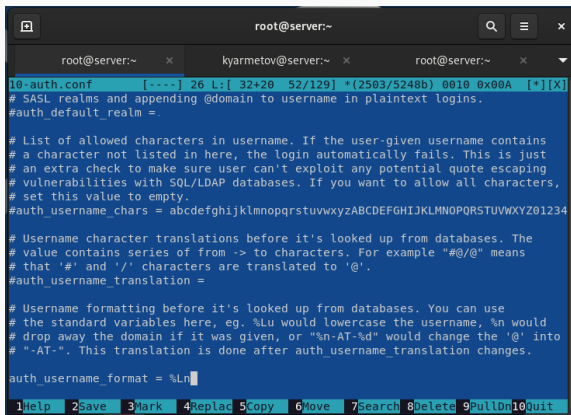
service submission-login {
  inet_listener submission {
    #port = 587
  }
}

service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    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.
```

Figure 2: файл 10-master.conf

Настройка LMTP в Dovecot



```
root@server:~  x  kyarmetov@server:~  x  root@server:~  x  ▾
10-auth.conf  [----] 26 L:[ 32+20  52/129] *(2503/5248b) 0010 0x00A [*][X]
# 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

# 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.

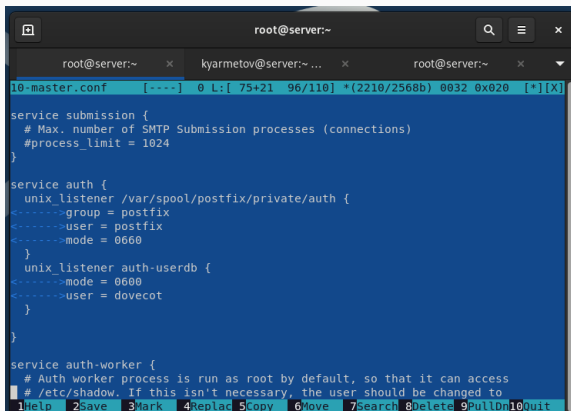
auth_username_format = %Ln
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

Figure 3: файл 10-auth.conf

```
n/server/mail/etc/postfix/  
[kyarmetov@server.kyarmetov.net ~]$  
[kyarmetov@server.kyarmetov.net ~]$ MAIL=~/.Maildir/mail  
s-nail version v14.9.22. Type '?' for help  
/home/kyarmetov/Maildir: 2 messages 1 new  
  1 kyarmetov      2023-02-17 13:52    18/642    "tt  
▶N  2 kyarmetov@client.kya  2023-02-17 14:09    21/838    "LMTP test  
& █
```

Figure 4: отправка письма

Настройка SMTP-аутентификации



The image shows a terminal window with a dark theme. The title bar at the top reads 'root@server:~'. Below the title bar, there are three tabs: 'root@server:~', 'kyarmetov@server:~...', and 'root@server:~'. The main content of the terminal is the configuration file '10-master.conf'. The configuration is as follows:

```
10-master.conf [----] 0 L:[ 75+21 96/110] *(2210/2568b) 0032 0x020 [*][X]

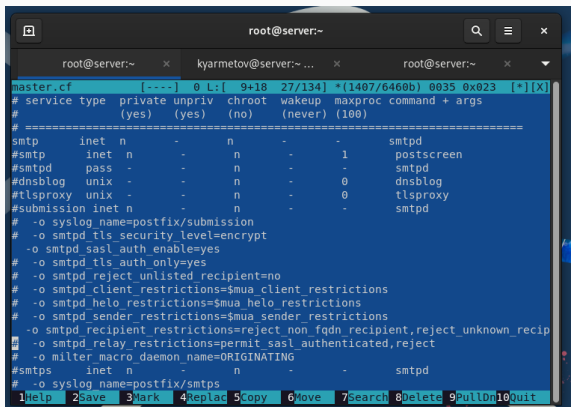
service submission {
    # Max. number of SMTP Submission processes (connections)
    #process_limit = 1024
}

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
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

Figure 5: файл 10-master.conf

Настройка SMTP-аутентификации



```
root@server:~  
master.cf [----] 0 L: [ 9+18 27/134] *(1407/6460b) 0035 0x023 [*][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  
#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=reject_non_fqdn_recipient,reject_unknown_recip  
-o smtpd_relay_restrictions=permit_sasl_authenticated,reject  
# -o milter_macro_daemon_name=ORIGINATING  
#smtps inet n - n - - smtpd  
# -o syslog_name=postfix/smtps  
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

Figure 6: файл master.cf

```
[kyarmetov@client.kyarmetov.net ~]$  
[kyarmetov@client.kyarmetov.net ~]$ printf 'kyarmetov\x00kyarmetov\x00123456' |  
base64  
a3lhcm1ldG92AGt5YXJtZXRvdGxMjM0NTY=  
[kyarmetov@client.kyarmetov.net ~]$ telnet server.kyarmetov.net 25  
Trying 192.168.1.1...  
Connected to server.kyarmetov.net.  
Escape character is '^]'.  
220 server.kyarmetov.net ESMTP Postfix  
AUTH PLAIN a3lhcm1ldG92AGt5YXJtZXRvdGxMjM0NTY=  
235 2.7.0 Authentication successful
```

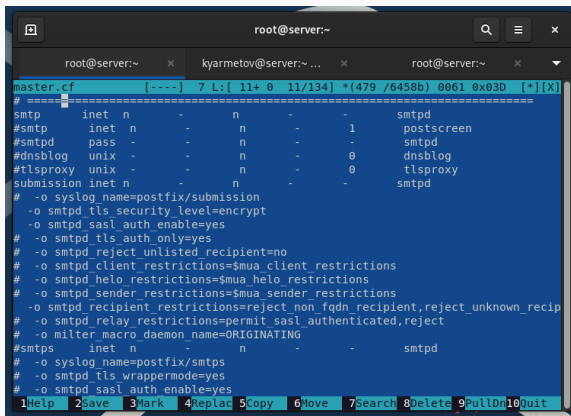
Figure 7: telnet авторизация

Настройка SMTP over TLS

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

Figure 8: конфигурация postfix

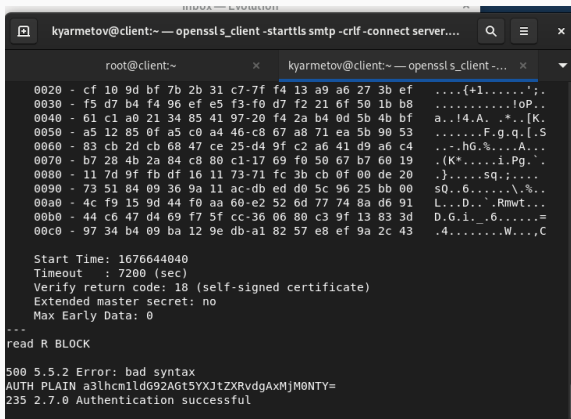
Настройка SMTP over TLS



```
root@server:~  
master.cf [----] 7 L: [ 11+ 0 11/134 ] *(479 /6458b) 0061 0x03D [*][X]  
# =====  
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=$mua_client_restrictions  
# -o smtpd_helo_restrictions=$mua_helo_restrictions  
# -o smtpd_sender_restrictions=$mua_sender_restrictions  
# -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recip  
# -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  
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

Figure 9: файл master.cf

Проверка работы



```
kyarmetov@client:~ — openssl s_client -starttls smtp -crlf -connect server....
root@client:~ x kyarmetov@client:~ — openssl s_client -... x
0020 - cf 10 9d bf 7b 2b 31 c7-7f f4 13 a9 a6 27 3b ef ....{+1.....';.
0030 - f5 d7 b4 f4 96 ef e5 f3-f0 d7 f2 21 6f 50 1b b8 .....!oP..
0040 - 61 c1 a0 21 34 85 41 97-20 f4 2a b4 0d 5b 4b bf a..!4.A. .*..[K.
0050 - a5 12 85 0f a5 c0 a4 46-c8 67 a8 71 ea 5b 90 53 .....F.g.q.[.S
0060 - 83 cb 2d cb 68 47 ce 25-d4 9f c2 a6 41 d9 a6 c4 ...-hG.%....A...
0070 - b7 28 4b 2a 84 c8 80 c1-17 69 f0 50 67 b7 60 19 ..(K*.....i.Pg.`
0080 - 11 7d 9f fb df 16 11 73-71 fc 3b cb 0f 00 de 20 ..}.....sq.;...
0090 - 73 51 84 09 36 9a 11 ac-db ed d0 5c 96 25 bb 00 sQ..6.....\%.
00a0 - 4c f9 15 9d 44 f0 aa 60-e2 52 6d 77 74 8a d6 91 L...D...`.Rmwt...
00b0 - 44 c6 47 d4 69 f7 5f cc-36 06 80 c3 9f 13 83 3d D.G.i...6.....=
00c0 - 97 34 b4 09 ba 12 9e db-a1 82 57 e8 ef 9a 2c 43 .4.....W....C

Start Time: 1676644040
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK

500 5.5.2 Error: bad syntax
AUTH PLAIN a3lhcm1ldG92AGt5YXJtZXRvdGxMjM0NTY=
235 2.7.0 Authentication successful
```

Figure 10: telnet авторизация

Проверка работы

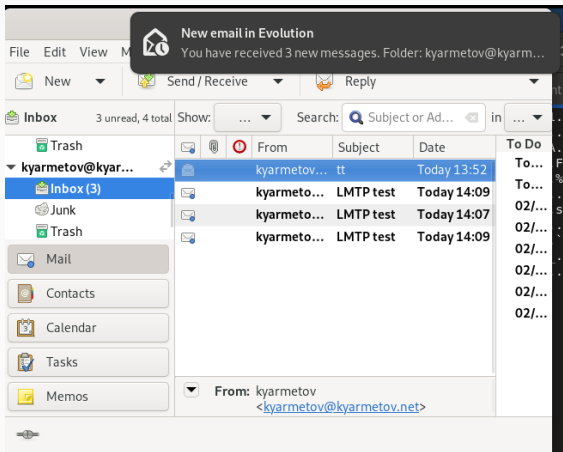


Figure 11: Работа почтового клиента

Приобретены практические навыки по установке и конфигурированию SMTP-сервера.