

Защита лабораторной работы № 10

Расширенные настройки SMTP-сервер

Администрирование сетевых подсистем

Работу Выполнил:
Саинт-Амур Измаэль
Группа: НПИбд-02-20



Цель работы

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

Установка Dovecot

```
saismael@server.saismael.net ~]$ sudo -i
[sudo] password for saismael:
[root@server.saismael.net ~]# dnf -y install dovecot telnet
Last metadata expiration check: 2:22:37 ago on Thu 08 Dec 2022 03:58:50 AM UTC
Dependencies resolved.
=====
Package            Arch      Version                               Repository  Size
=====
Installing:
dovecot            x86_64    1:2.3.16-7.el9                       appstream   4.7
telnet             x86_64    1:0.17-85.el9                        appstream   63
Installing dependencies:
clucene-core       x86_64    2.3.3.4-42.20130812.e8e3d20git.el9    appstream   585
libexttextcat      x86_64    3.4.5-11.el9                         appstream   209
Transaction Summary
=====
Install 4 Packages

Total download size: 5.6 M
Installed size: 20 M
Downloading Packages:
(1/4): telnet-0.17-85.el9.x86_64.rpm 43 kB/s | 63 kB 00:01
(2/4): libexttextcat-3.4.5-11.el9.x86_64.rpm 142 kB/s | 209 kB 00:01
```

Добавляем в список протоколов, с которыми может работать Dovecot, протокол LMTP. Настраиваем в Dovecot сервис lmtp для связи с Postfix. Переопределяем в Postfix с помощью postconf передачу сообщений не на прямую, а через задан

```
/etc/dovecot/dovecot.conf 1799/
# Paths are also just examples with the real defaults being
# options. The paths listed here are for configure --prefix
# --sysconfdir=/etc --localstatedir=/var

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

```
10-master.conf  [----] 16 L:[ 45+10 55/133] *(1391/3643b) 0032 0x020 [*][X]
}
}

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

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 =
  #}
}
```

1 Help 2 Save 3 Mark 4 Replace 5 Copy 6 Move 7 Search 8 Delete 9 PullDn 10 Quit


```
[root@server.saismael.net ~]# systemctl restart postfix
[root@server.saismael.net ~]# systemctl restart dovecot
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# echo . | mail -s "LMTP test"saismael@saismael.net
s-nail: Send options without primary recipient specified.
mail (s-nail v14.9.22): send and receive Internet mail
Send-only mode: send mail "to-addr"(ess) receiver(s):
  mail [-DdEFInv~#] [-: spec] [-A account] [:-C "field: body":]
    [:-a attachment:] [:-b bcc-addr:] [:-c cc-addr:]
    [-M type | -m file | -q file | -t] [-r from-addr] [:-S var[=value]:]
    [-s subject] [-T "arget: addr"] [:-X/Y cmd:] [-.] :to-addr:
"Receive" mode, starting on [-u user], primary *inbox* or [$MAIL]:
  mail [-DdEeHiNnRv~#] [-: spec] [-A account] [:-C "field: body":]
    [-L spec] [-r from-addr] [:-S var[=value]:] [-u user] [:-X/Y cmd:]
"Receive" mode, starting on -f (secondary $MBOX or [file]):
  mail [-DdEeHiNnRv~#] [-: spec] [-A account] [:-C "field: body":] -f
    [-L spec] [-r from-addr] [:-S var[=value]:] [:-X/Y cmd:] [file]
. -d sandbox, -: / no .rc files, -. end options and force send-mode
```

- определяем службу аутентификации пользователей
- задаем тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету
- Настраиваем Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины

```
10-master.conf  [----] 16 L:[ 45+10  55/133] *(1391/3643b) 0032 0x020 [*][X]
}
}

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

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 =
  }
}

[root@server.saismael.net ~]# MAIL=~/.Maildir/ mail
s-nail: No mail for root at /root/Maildir/
s-nail: /root/Maildir/: No such entry, file or directory
[root@server.saismael.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.saismael.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# postconf -e 'smtpd_recipient_restrictions = reject_unkown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'
[root@server.saismael.net ~]#
```


- указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности.
- Изменяем файл `/etc/postfix/master.cf` для того чтобы запустить SMTP-сервер на 587 порту
- Настраиваем межсетевой экран, разрешив работать службе `smtp-submission`

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

```
master.cf  [-M--]  0 L: [ 15+ 4 19/134] *(973 /6459b) 0032 0x020 [*][X]  
#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=$mua_sender_restrictions  
#  -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_address  
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject  
#  -o milter_macro_daemon_name=ORIGINATING  
#smtps     inet  n  -  n  -  -  smtpd  
#  -o syslog_name=postfix/smtps  
#  -o smtpd_tls_wrappermode=yes  
#  -o smtpd_sasl_auth_enable=yes  
#  -o smtpd_reject_unlisted_recipient=no  
#  -o smtpd_client_restrictions=$mua_client_restrictions  
#  -o smtpd_helo_restrictions=$mua_helo_restrictions  
#  -o smtpd_sender_restrictions=$mua_sender_restrictions  
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

Настройка SMTP over TLS

Sending Email

Welcome
entity
ceiving Email
ceiving Options
nding Email
count Summary
one

Server Type: SMTP

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

Configuration

Server: mail.saisamel.net Port: 587

☒ Server requires authentication

Security

Encryption method: STARTTLS after connecting

Authentication

Type: Check for Supported Types

Username: saismael

PLAIN
NTLM / SPA
GSSAPI
DIGEST-MD5
CRAM-MD5
Login
POP before SMTP

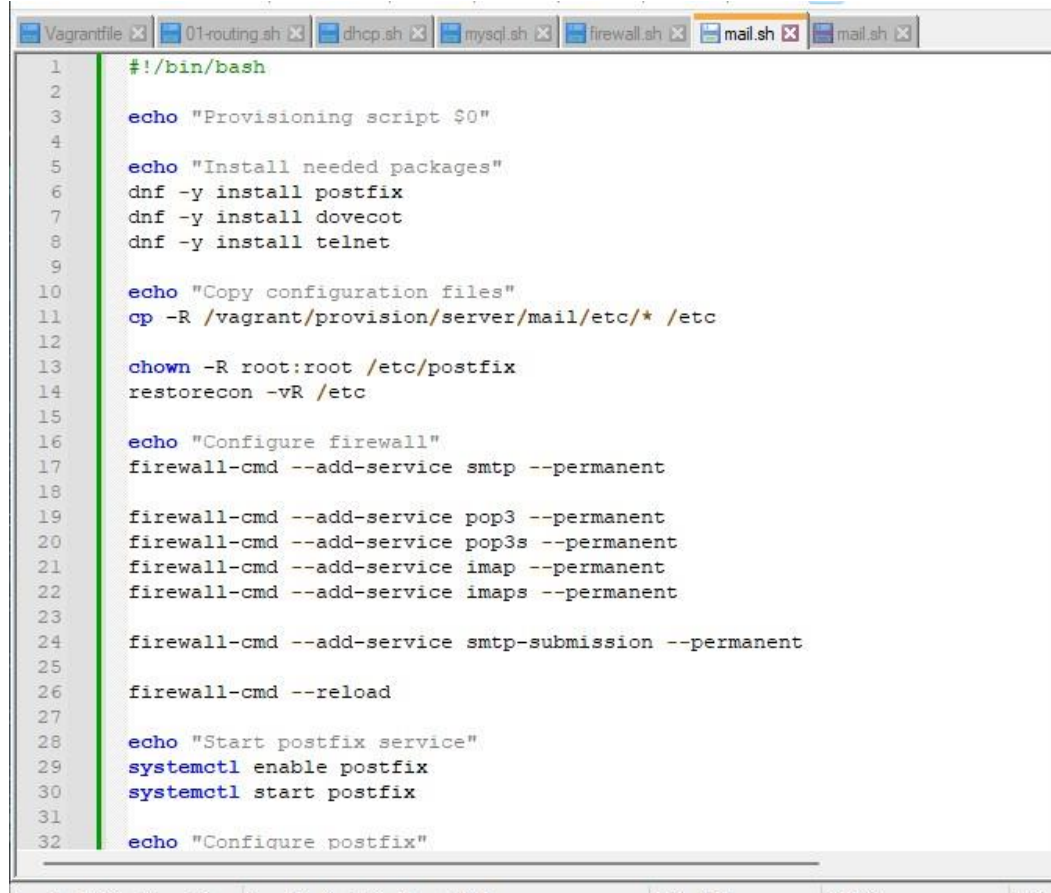
Back Next

Right Ctrl

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
[root@server.saismael.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.saismael.net server]# cp -R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postfix/
```

```
[root@server.saismael.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.saismael.net server]# cp -R /etc/dovecot/conf.d/10-master.conf /vagrant/provision/server/mail/etc/dovecot/conf.d/
```

A screenshot of a terminal window with a light gray title bar containing several open tabs: 'Vagrantfile', '01-routing.sh', 'dhcp.sh', 'mysql.sh', 'firewall.sh', 'mail.sh', and 'mail.sh'. The terminal content shows a shell script with line numbers 1 through 32. The script includes comments and commands for installing postfix, dovecot, and telnet; copying configuration files from /etc to /vagrant; setting permissions; configuring the firewall to allow SMTP, POP3, and IMAP; and enabling the postfix service.

```
1  #!/bin/bash  
2  
3  echo "Provisioning script $0"  
4  
5  echo "Install needed packages"  
6  dnf -y install postfix  
7  dnf -y install dovecot  
8  dnf -y install telnet  
9  
10 echo "Copy configuration files"  
11 cp -R /vagrant/provision/server/mail/etc/* /etc  
12  
13 chown -R root:root /etc/postfix  
14 restorecon -vR /etc  
15  
16 echo "Configure firewall"  
17 firewall-cmd --add-service smtp --permanent  
18  
19 firewall-cmd --add-service pop3 --permanent  
20 firewall-cmd --add-service pop3s --permanent  
21 firewall-cmd --add-service imap --permanent  
22 firewall-cmd --add-service imaps --permanent  
23  
24 firewall-cmd --add-service smtp-submission --permanent  
25  
26 firewall-cmd --reload  
27  
28 echo "Start postfix service"  
29 systemctl enable postfix  
30 systemctl start postfix  
31  
32 echo "Configure postfix"
```

Приобрел практические навыки по
конфигурированию SMTP-сервера в части настройки
аутентификации.