

Презентация лабораторной работы №10

Бакулин Никита 1032201747

Цель работы

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

Задачи

- Настройте Dovecot для работы с LMTP
- Настройте аутентификацию посредством SASL на SMTP-сервере
- Настройте работу SMTP-сервера поверх TLS
- Скорректируйте скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server

Результаты выполнения

- Настройте Dovecot для работы с LMTP

```
# 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
```

Рис. 1

```
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 =
    #}
}
```

Рис. 2

```
[root@server.nabakulin.net ~]# postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'
[root@server.nabakulin.net ~]# systemctl restart postfix
[root@server.nabakulin.net ~]# systemctl restart dovecot
[root@server.nabakulin.net ~]# exit
logout
[nabakulin@server.nabakulin.net ~]$ echo .| mail -s "LMTP test" nabakulin@nabakulin.net
[nabakulin@server.nabakulin.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/nabakulin/Maildir: 5 messages 1 new 3 deleted
 4 nabakulin      2022-12-10 19:48  18/645  "test
+N 5 nabakulin@nabakulin. 2022-12-11 00:20  18/608  "LMTP test
& exit
[nabakulin@server.nabakulin.net ~]$

root@server:~
d)
Dec 11 00:20:26 server postfix/pickup[8112]: 4E73584BAB4: uid=1001 from=<nabakulin>
Dec 11 00:20:26 server postfix/cleanup[8137]: 4E73584BAB4: message-id=<20221211002026.4E73584BAB4@server.nabakulin.net>
Dec 11 00:20:26 server postfix/qmgr[8113]: 4E73584BAB4: from=<nabakulin@nabakulin.net>, size=335, nrcpt=1 (queue active)
Dec 11 00:20:26 server dovecot[8124]: lmtp(8145): Connect from local
Dec 11 00:20:26 server dovecot[8124]: lmtp(nabakulin)<8145></Ze4JEoilWPRHwAAfWBhbg>: msgid=<20221211002026.4E73584BAB4@server.nabakulin.net>; saved mail to INBOX
Dec 11 00:20:26 server postfix/lmtp[8144]: 4E73584BAB4: to=<nabakulin@nabakulin.net>, relay=server.nabakulin.net[private/dovecot-lmtp], delay=0.51, delays=0.05/0.13/0.15/0.18, dsn=2.0.0, status=sent (250 2.0.0 <nabakulin@nabakulin.net> /Ze4JEoilWPRHwAAfWBhbg Saved)
Dec 11 00:20:26 server postfix/qmgr[8113]: 4E73584BAB4: removed
Dec 11 00:20:26 server dovecot[8124]: lmtp(8145): Disconnect from local: Logged out (state=READY)
```

Рис. 3

Результаты выполнения

- Настройте аутентификацию посредством SASL на SMTP-сервере

```
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.
#
# The default 0666 mode allows anyone to connect to the socket, but the
# userdb lookups will succeed only if the userdb returns an "uid" field that
# matches the caller process's UID. Also if caller's uid or gid matches the
# socket's uid or gid the lookup succeeds. Anything else causes a failure.
#
# To give the caller full permissions to lookup all users, set the mode to
# something else than 0666 and Dovecot lets the kernel enforce the
# permissions (e.g. 0777 allows everyone full permissions).
unix_listener auth-userdb {
mode = 0600
user = dovecot
#group =
}

# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
group = postfix
user = postfix
mode = 0600
}

# Auth process is run as this user.
#user = $default_internal_user
}
```

Рис. 4

```
# =====
# service type private unpriv chroot wakeup maxproc command + args
# (yes) (yes) (no) (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
```

Рис. 5

```
[root@server.nabakulin.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.nabakulin.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.nabakulin.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.nabakulin.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'
[root@server.nabakulin.net ~]# vi /etc/postfix/master.cf
[root@server.nabakulin.net ~]# systemctl restart postfix
[root@server.nabakulin.net ~]# systemctl restart dovecot
Job for dovecot.service failed because the control process exited with error code.
See "systemctl status dovecot.service" and "journalctl -xeu dovecot.service" for details.
[root@server.nabakulin.net ~]# systemctl restart dovecot
```

Рис. 6

```
[root@client.nabakulin.net ~]# printf 'nabakulin\x00nabakulin\x00password' | base64
bmFiYWt1bGluAG5hYmFrdWxpbGwYXNzd29yZA==
[root@client.nabakulin.net ~]# telnet server.nabakulin.net 25
Trying 192.168.1.1...
Connected to server.nabakulin.net.
Escape character is '^]'.
220 server.nabakulin.net ESMTP Postfix
EHLO test
250-server.nabakulin.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 bmFiYWt1bGluAG5hYmFrdWxpbGwYXNzd29yZA==
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Рис. 7

Результаты выполнения

- Настройте работу SMTP-сервера поверх TLS

```
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - ff f1 eb 58 3c 69 74 b2-de 62 43 4d b2 0b 73 32 ...X<it..bCM..s2
0010 - 24 ee 80 f9 69 49 0a 78-12 8a 51 da c6 10 17 eb $...iI.X..Q....
0020 - 66 16 24 e1 eb c1 e2 93-26 7e 46 85 67 ec bf 0b f.$.....&~F.g...
0030 - 1a 7e 7a 81 30 fc cc f6-89 c7 e7 d5 90 f3 e4 83 .~z.0.....
0040 - 8e 69 1a d1 14 07 6b e9-28 ef 75 49 e0 20 c0 4c .i....k.(.uI. .L
0050 - 74 dd 73 a5 12 ac a9 7c-dd 5d c9 b5 11 76 df 02 t.s....[.]...v..
0060 - a3 01 d2 4d 94 f8 62 7f-53 20 18 e2 17 7f 28 99 ...M..b.S ....(
0070 - 19 a6 61 82 c4 c7 de ab-15 24 e7 53 3f 65 58 4d ..a.....$.S?eXM
0080 - d8 a7 84 77 0d e6 28 bd-9a 88 36 61 27 32 dd a1 ...w..(...6a'2..
0090 - ac 37 eb 72 c6 a8 9d 2a-59 15 07 fc 9b 6a 13 4d .7.r...*Y....j.M
00a0 - 7b 1c 31 60 01 16 32 88-98 cd 9e 84 a7 1e c3 ed {.1`.2.....
00b0 - 22 db 67 19 c4 82 db 9f-35 3e f9 4c a4 32 c0 70 ".g....5>.L.2.p
00c0 - 64 36 7f d9 aa 4c 21 ee-45 4d 58 88 c8 cb 93 2f d6...L!.EMX..../

Start Time: 1670719002
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.nabakulin.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 bmFiYwt1bGluAG5hYmFrdWxpbGwYXNzd29yZA==
235 2.7.0 Authentication successful
```

Рис. 8

```
# =====
# 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 smtpd_sasl_auth_enable=yes -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
```

Рис. 9

Server Type: SMTP

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

Configuration

Server: mail.nabakulin.net Port: 587

☒ Server requires authentication

Security

Encryption method: STARTTLS after connecting

Authentication

Type: Check for Supported Types PLAIN

Username: nabakulin

Рис. 10

	nabakulin <nabakulin@...>	test	Yesterday 19:48
	nabakulin@nabakulin....	LMTP test	Today 00:20
	nabakulin <nabakulin@...>	test tls	Today 00:39

Рис. 11

Результаты выполнения

- Скорректируйте скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server

```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install postfix
dnf -y install s-nail
dnf -y install dovecot telnet

echo "Copy configuration files"
cp -R /vagrant/provision/server/mail/etc/* /etc
chown -R root:root /etc/postfix
restorecon -VR /etc

echo "Configure firewall"
firewall-cmd --add-service=smtp --permanent
firewall-cmd --add-service=pop3 --permanent
firewall-cmd --add-service=pop3s --permanent
firewall-cmd --add-service=imap --permanent
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 = nabukulin.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_mynetworks, reject_non_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_files=/etc/pki/tls/certs/dovecot.pem'
postconf -e 'smtpd_tls_key_files=/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

systemctl stop postfix
systemctl start postfix
systemctl restart dovecot
```

Рис. 10

```
#!/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. 11