

Отчёт о лабораторной работе

Лабораторная работа 10

Мантуров Татархан Бесланович

Содержание

Цель работы

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

Выполнение лабораторной работы

Во втором терминале сервера запустим вывод логов почты (рис. [-@fig:001]).

```
[tbanturov@server.tbanturov.net ~]$ sudo -i
[sudo] password for tbanturov:
[root@server.tbanturov.net ~]# tail -f /var/log/maillog
Feb  2 22:48:49 server postfix/postalias[1470]: warning: unsupported dictionary type: hash. Is the postfix-hash package installed?
Feb  2 22:48:49 server postfix/postalias[1470]: fatal: unsupported map type: hash
Feb  2 22:48:51 server postfix[1552]: Postfix is using backwards-compatible default settings
Feb  2 22:48:51 server postfix[1552]: See http://www.postfix.org/COMPATIBILITY_README.html for details
Feb  2 22:48:51 server postfix[1552]: To disable backwards compatibility use "postconf compatibility_level=3.6" and "postfix reload"
Feb  2 22:48:51 server postfix-script[1624]: starting the Postfix mail system
Feb  2 22:48:51 server postfix/master[1627]: daemon started -- version 3.8.5, configuration /etc/postfix
Feb  2 22:49:22 server dovecot[1677]: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3
```

Логи почты /var/log/maillog

В первом же терминале сервера авторизуемся под рутом и откроем файл конфигурации /etc/dovecot/dovecot.conf.

В этом файле допишем в список рабочих протоколов протокол lmtp (рис. [-@fig:003]).

```
!include_try local.conf
protocols = imap pop3 lmtp
```

/etc/dovecot/dovecot.conf

Далее, откроем конфигурационный файл /etc/dovecot/conf.d/10-master.conf. Внутри этого файла пропишем следующее тело для структуры service lmtp (рис. [-@fig:005]).

```

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

```

service lmtp

Далее, пропишем в postfix сокет, через который будет идти отправка сообщений. После этого откроем файл /etc/dovecot/conf.d/10-auth.conf (рис. [-@fig:006]).

```
[root@server.tbmanturov.net ~]# postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'
```

Настройка сокета

В этом файле зададим значение для поля auth_username_format, отвечающее за формат имени пользователя для аутентификации. В нашем случае домен не будет указываться (рис. [-@fig:007]).

```
#auth_username_format = %Ln
```

auth_username_format

Перезапустим postfix и dovecot (рис. [-@fig:008]).

```
[root@server.tbmanturov.net ~]# systemctl restart dovecot
[root@server.tbmanturov.net ~]# systemctl restart postfix

```

Перезапуск postfix и dovecot

Теперь перейдём на виртуальную машину клиента. Попробуем отправить письмо самому себе (рис. [-@fig:009]).

```
[root@client.tbmanturov.net client]# echo . | mail -s "LMTP test" tbmanturov@tbmanturov.net
[root@client.tbmanturov.net client]#
```

Отправка письма

В логах, которые мы открывали на сервере в самом начале выполнения лабораторной работы, мы видим, что письмо было доставлено в ящик. Об этом свидетельствует подпись “saved mail to INBOX”. Кроме того, теперь в логах пишется, что транспортировка осуществляется через lmtp (passing ... to transport=lmtp) (рис. [-@fig:010]).

```

[tbmanturov@server.tbmanturov.net ~]$ sudo -i
[sudo] password for tbmanturov:
[root@server.tbmanturov.net ~]# tail -f /var/log/maillog
Feb  2 22:48:49 server postfix/postalias[1470]: warning: unsupported dictionary type: hash. Is the postfix-hash packa
ge installed?
Feb  2 22:48:49 server postfix/postalias[1470]: fatal: unsupported map type: hash
Feb  2 22:48:51 server postfix[1552]: Postfix is using backwards-compatible default settings
Feb  2 22:48:51 server postfix[1552]: See http://www.postfix.org/COMPATIBILITY_README.html for details
Feb  2 22:48:51 server postfix[1552]: To disable backwards compatibility use "postconf compatibility_level=3.6" and "
postfix reload"
Feb  2 22:48:51 server postfix/postfix-script[1624]: starting the Postfix mail system
Feb  2 22:48:51 server postfix/master[1627]: daemon started -- version 3.8.5, configuration /etc/postfix
Feb  2 22:49:22 server dovecot[1677]: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3

```

Логи почты

Откроем на сервере почтовый ящик, чтобы убедиться, что письмо успешно доставлено. Как видим, это действительно так (рис. [-@fig:011]).

```
Feb  2 23:29:23 server postfix/smtp[11416]: connect to mail.tbmanturov.net[192.168.1.1]:25: Connection refused
Feb  2 23:29:23 server postfix/smtp[11416]: 23019193f48: to=<tbmanturov@tbmanturov.net>, relay=none, delay=2.1, delay
s=0.03/0.01/2/0, dsn=4.4.1, status=deferred (connect to mail.tbmanturov.net[192.168.1.1]:25: Connection refused)
```

Почтовый ящик mail

Теперь откроем файл конфигурации по пути `/etc/dovecot/conf.d/10-master.conf`.

Приведем содержание тела структуры `service auth` к следующему виду. Разберём построчно

`service auth { ... }` - Эта строка объявляет начало секции конфигурации для внутренней службы Dovecot, которая называется `auth`.

`unix_listener /var/spool/postfix/private/auth { ... }` - Указывает Dovecot создать "слушателя" на основе UNIX-сокета.

`group = postfix` - Устанавливает группу-владельца для файла сокета.

`user = postfix` - Устанавливает пользователя-владельца для файла сокета.

`mode = 0660` - Устанавливает права доступа к файлу сокета в восьмеричном формате.

`unix_listener auth-userdb { ... }` - Создает второй UNIX-сокет.

`mode = 0600` - Устанавливает права доступа для этого внутреннего сокета.

`user = dovecot` - Устанавливает пользователя-владельца `dovecot`.

(рис. [-@fig:013]).

```
GNU nano 8.1 /etc/dovecot/conf.d/10-master.conf Modified
#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
    }
    # 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 {
    #    mode = 0666
    #}

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

Структура service auth

Теперь настроим аутентификацию почты `smtp` для `postfix` и укажем, каким правилам следовать для работы с почтой и её фильтрации. Рассмотрим опции

`reject_unknown_recipient_domain` - Отклонить письмо, если домен в адресе получателя не существует.

`permit_mynetworks` - Разрешить письмо без дальнейших проверок, если IP-адрес

клиента, отправляющего письмо, находится в списке доверенных сетей.

`reject_non_fqdn_recipient` - Отклонить письмо, если адрес получателя не является полностью определённым доменным именем.

`reject_unauth_destination` - отклоняет письмо, если домен получателя не является локальным для этого сервера и при этом сессия не аутентифицирована.

`reject_unverified_recipient` - Отклонить письмо, если Postfix не может проверить существование получателя.

`permit` - Если ни одно из предыдущих правил не отклонило и не разрешило письмо, это правило разрешает его.

(рис. [-@fig:014]).

```
[root@server.tbanturov.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.tbanturov.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.tbanturov.net ~]# nano /etc/dovecot/conf.d/10-master.conf
[root@server.tbanturov.net ~]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks'
```

Настройка почты в postfix

Теперь отредактируем файл `/etc/postfix/master.cf`.

В этом файле внесём изменения так, чтобы smtp поддерживал авторизацию по sasl (рис. [-@fig:016]).

```
GNU nano 8.1 /etc/postfix/master.cf
#
# 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_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated
#smtp inet n - n - - 1 postscreen
#smtpd pass - - - - - smtpd
#dnsblog unix - - n - 0 dnsblog
#tlsproxy unix - - n - 0 tlsproxy
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n - n - - smtpd
#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 local_header_rewrite_clients=static:all
# -o smtpd_reject_unlisted_recipient=no
#
# Instead of specifying complex smtpd_<xxx>_restrictions here,
# specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
# here, and specify mua_<xxx>_restrictions in main.cf (where
# "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
#
# -o smtpd_client_restrictions=
# -o smtpd_helo_restrictions=
# -o smtpd_sender_restrictions=
# -o smtpd_relay_restrictions=
# -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
# Choose one: enable submissions for loopback clients only, or for any client.
#127.0.0.1:submissions inet n - n - - smtpd
#submissions inet n - n - - smtpd
#
# -o syslog_name=postfix/submissions
# -o smtpd_tls_wrappermode=yes
# -o smtpd_sasl_auth_enable=yes
```

Включение авторизации

Теперь перезапустим postfix и dovecot (рис. [-@fig:017]).

```
[root@server.tbanturov.net ~]# systemctl restart dovecot
[root@server.tbanturov.net ~]# systemctl restart postfix
```

Перезапуск postfix и dovecot

Теперь на клиенте установим telnet (рис. [-@fig:018]).

Установка Telnet

```
[root@client.tbmanturov.net ~]# printf 'tbmanturov\x00tbmanturov\x001234' | base64
dGJtYW50dXJvdG80Ym1hbnR1cm92ADEyMzQ=
```

```
telnet: connect to address 192.168.1.1: connection refused
[root@client.tbmanturov.net ~]# telnet server.tbmanturov.net 25
Trying 192.168.1.1...
```

```
# =====
smtp      inet n       -       n       -       -       smtpd

submission inet n - - - smtpd
-o smtpd_tls_security_level=encrypt
-o smtpd_sasl_auth_enable=yes
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_j
n_recipient_domain,permit_sasl_authenticated,reject
```

[illegible]

```
[root@client.tbmanturov.net ~]# openssl s_client -starttls smtp -crlf -connect server.tbmanturov.net:587
C0527E00BD7F0000:error:8000006F:system library:BIO_connect:Connection refused:crypto/bio/bio_sock2.c:178:connect()
C0527E00BD7F0000:error:10000067:BIO routines:BIO_connect:connect error:crypto/bio/bio_sock2.c:180:
connect:errno=111
[root@client.tbmanturov.net ~]#
```

openssl

Теперь сохраним внесённые нами изменения в vagrant (рис. [-@fig:029]).

```
[root@server.tbmanturov.net ~]# cd /vagrant/provision/server
[root@server.tbmanturov.net server]# cp -R /etc/dovecot/dovecot.conf /vagrant/provision/server/mail/etc/dovecot/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/dovecot.conf'? yes
[root@server.tbmanturov.net server]# cp -R /etc/dovecot/conf.d/10-master.conf /vagrant/provision/server/mail/etc/dovecot/conf.d/
[root@server.tbmanturov.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'? yes
[root@server.tbmanturov.net server]# mkdir -p /vagrant/provision/server/mail/etc/postfix/
[root@server.tbmanturov.net server]#
```

vagrant

На сервере изменим скрипт mail.sh следующим образом (рис. [-@fig:030]).

```
root@server:~ - sudo -i
root@server:/vagrant/provision/server - sudo -i

GNU nano 8.1 mail.sh
#!/bin/bash
echo "Provisioning script $@"
echo "Install needed packages"
dnf -y install postfix
dnf -y install s-nail
echo "Copy configuration files"
#cp -R /vagrant/provision/server/mail/etc/* /etc
echo "Configure firewall"
firewall-cmd --add-service-smtp --permanent
firewall-cmd --reload
restorecon -vR /etc
echo "Start postfix service"
systemctl enable postfix
systemctl start postfix
echo "Configure postfix"
postconf -e 'mydomain = user.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'
postfix set-permissions
restorecon -vR /etc
systemctl stop postfix
systemctl start postfix
dnf -y install dovecot telnet
firewall-cmd --get-services
firewall-cmd --add-service-pop3 --permanent
firewall-cmd --add-service-pop3s --permanent
firewall-cmd --add-service-imaps --permanent
firewall-cmd --add-service-imaps --permanent
firewall-cmd --reload
firewall-cmd --list-services
postconf -e 'home_mailbox = Maildir/'
systemctl restart postfix
systemctl enable dovecot
```

mail.sh для сервера

Выводы

В результате выполнения лабораторной работы были получены навыки продвинутой настройки smtp и авторизации