Отчёт о лабораторной работе

Лабораторная работа 10

Мантуров Татархан Бесланович

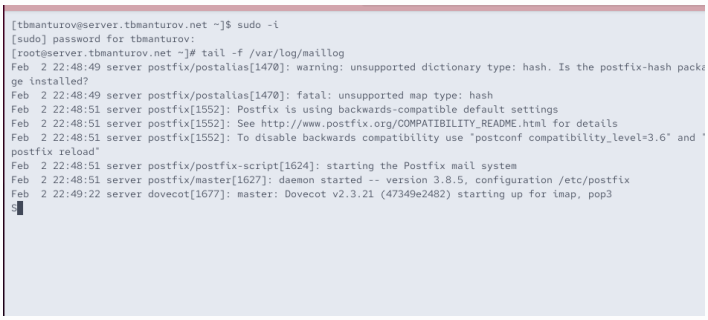
Содержание

Цель работы

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

Выполнение лабораторной работы

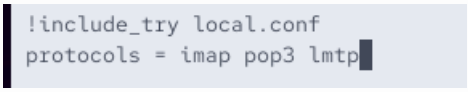
Во втором терминале сервера запустим вывод логов почты (рис. [-@fig:001]).



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]).



/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]#
```

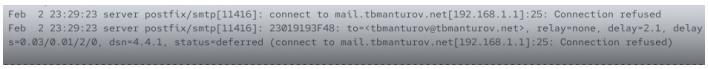
Отправка письма

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 lmap, pop3
s
```

Логи почты

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



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]).

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

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>
#smtp      inet  n       -       n       -       1       postscreen
#smtpd     pass  -       -       n       -       -       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]).

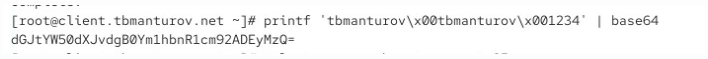
```
[root@server.tbmanturov.net ~]# systemctl restart dovecot
[root@server.tbmanturov.net ~]# systemctl restart postfix
[root@server.tbmanturov.net ~]#
```

Перезапуск postfix и dovecot

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

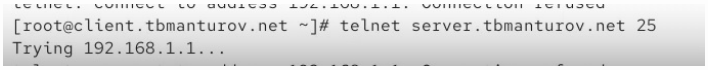
Установка Telnet

Теперь получим ключ авторизации. Этот ключ представляет из себя строку, содержащую имя пользователя и пароль, и зашифрованную в base64. Теперь по telnet подключимся к почтовому серверу и проверим соединение. После этого попробуем с помощью команды auth авторизироваться, в качестве ключа используя нашу base64 строку. Как видим, авторизация прошла успешно (Authentification successful) (рис. [-@fig:019]).



Авторизация по telnet

Теперь настроим сертификаты для postfix, а также уровень security и путь к базе данных кэша (рис. [-@fig:020]).

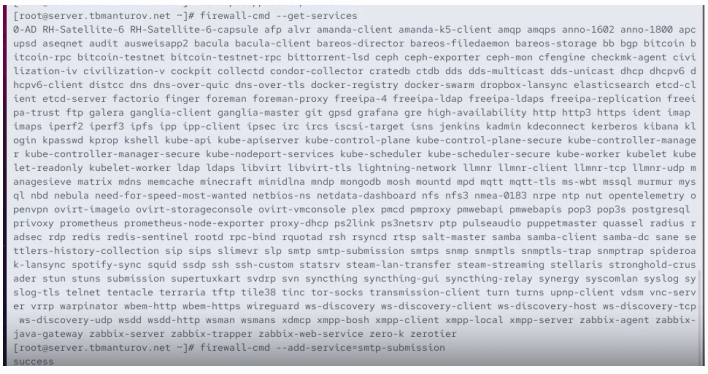


Настройка postfix

Вновь откроем файл /etc/postfix/master.cf и изменим его следующим образом (рис. [-@fig:021]).

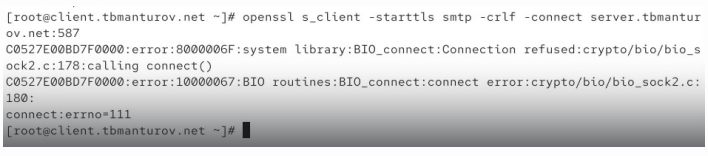
/etc/postfix/master.cf

Теперь настроим firewall, разрешив использовать smtp-submission, и перезапустим postfix (рис. [-@fig:022]).



Настройка firewall

Теперь подключимся к серверу через openssl (рис. [-@fig:023]).

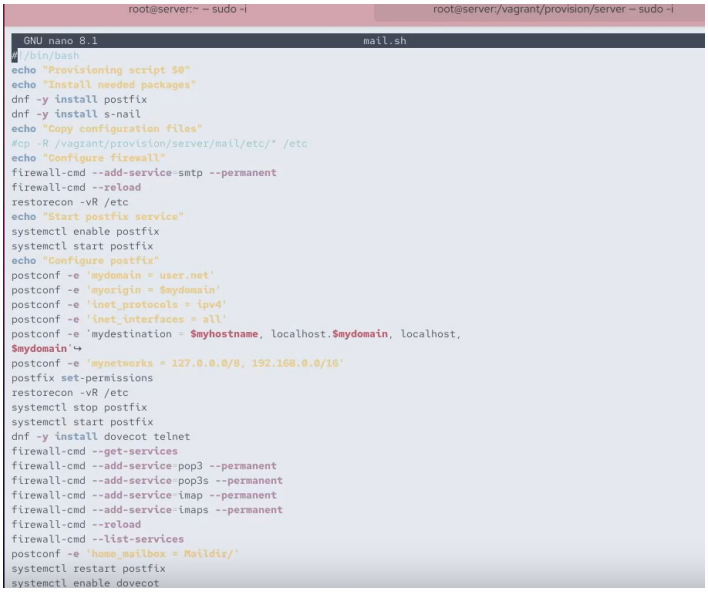


openssl

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

vagrant

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



mail.sh для сервера

Выводы

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