

# Расширенные настройки SMTP-сервера

---

Абд эль хай мохамад

РУДН, Москва, Российская Федерация

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

# Задачи

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

# Выполнение задачи

```
root@server:~  
[maabedelhay@server.maabedelhay.net ~]$ echo .| mail -s "LMTP test" maabedelhay@maabedelhay.net  
[maabedelhay@server.maabedelhay.net ~]$ echo .| mail -s "LMTP test2" maabedelhay@maabedelhay.net  
[maabedelhay@server.maabedelhay.net ~]$ MAIL=~/.Maildir/ mail  
s-nail version v14.9.22. Type '?' for help  
/home/maabedelhay/Maildir: 4 messages 2 new  
1 maabedelhay@client.m 2023-12-07 00:18 17/707 "test19  
2 maabedelhay@client.m 2023-12-07 00:24 17/723 "test20  
N 3 maabedelhay@maabedel 2023-12-08 13:07 18/640 "LMTP test  
N 4 maabedelhay@maabedel 2023-12-08 14:29 18/641 "LMTP test2  
& █
```

Отправил письмо с помощью утилиты mail с заголовком «test», а затем просмотрел папку «Входящие» с помощью команды MAIL=~/.Maildir/mail.

```
root@server:/vagrant/provision/client  
GNU nano 5.6.1 /etc/dovecot/dovecot.conf  
# and tabs are ignored. If you want to use either of these explicitly, put the  
# value inside quotes, eg.: key = "# char and trailing whitespace "  
  
# Most (but not all) settings can be overridden by different protocols and/or  
# 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█  
  
# 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,
```

Добавлен протокол smtp



# Выполнение задачи

`service auth {`: Эта строка указывает на начало блока конфигурации службы аутентификации.

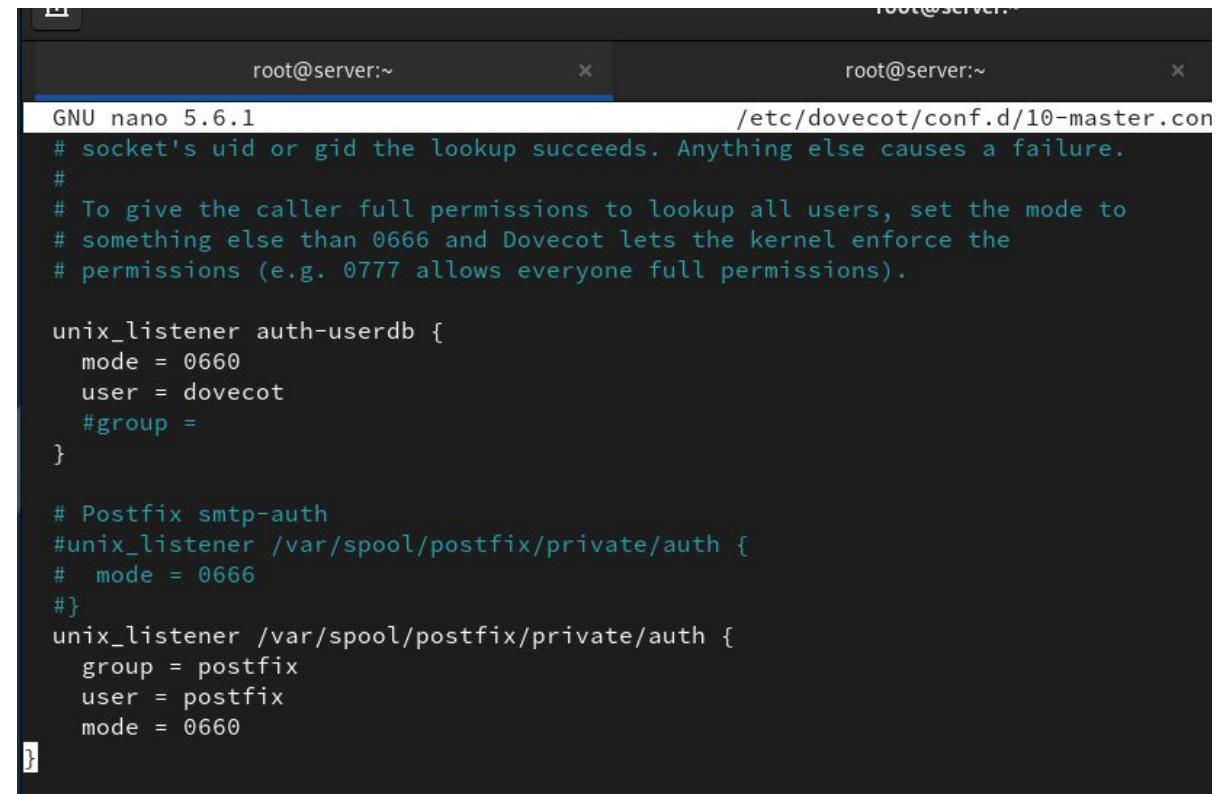
`unix_listener /var/spool/postfix/private/auth {`: Эта строка определяет файл сокета Unix, который будет прослушивать служба аутентификации. В данном случае путь к файлу — `/var/spool/postfix/private/auth`.

`mode = 0660`: Эта строка устанавливает разрешения файла сокета Unix на 0660, что означает, что владелец и группа имеют разрешения на чтение и запись, в то время как другие не имеют разрешений.

`unix_listener auth-userdb {`: Эта строка указывает другой файл сокета Unix, который будет прослушивать служба аутентификации. В данном случае имя файла — `auth-userdb`.

`mode = 0600`: Эта строка устанавливает права доступа к файлу сокета Unix `auth-userdb` равным 0600, что означает, что только владелец имеет разрешения на чтение и запись, в то время как другие не имеют разрешений.

`user = dovecot`: эта строка устанавливает право собственности на файл сокета Unix `auth-userdb` пользователю `dovecot`.



```
GNU nano 5.6.1 /etc/dovecot/conf.d/10-master.conf
# 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 = 0660
  user = dovecot
  #group =
}

# Postfix smtp-auth
#unix_listener /var/spool/postfix/private/auth {
#  mode = 0666
#}
unix_listener /var/spool/postfix/private/auth {
  group = postfix
  user = postfix
  mode = 0660
}
```

# Выполнение задачи

На клиенте я подключился к SMTP-серверу через порт 587, используя openssl :  
openssl s\_client -starttls smtp -crlf -connect server.maabedelhay.net:587

```
maabedelhay@client:~ — openssl s_client -starttls smtp -crlf -c
---
250 CHUNKING
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: CB7C5F17F67A26666DC00C12EDC32EF09D3D9D9FD8488E8F454A425C5FC87677
    Session-ID-ctx:
    Resumption PSK: F038F03322D2ABB5D1B4060236C75F92A2E97B31E367DBED4391CF2A7B22449421241A8B9AF3DC6E379D93C067479FA2
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 17 3d 76 25 57 4a 87 c4-8f 7b 5d f1 ec 35 63 ee      .:=v%WJ...{[]..5c.
    0010 - 79 0c 04 cc 8a 42 da 18-2e 44 ce e3 59 1f 98 43      y....B...D..Y..C
    0020 - 38 90 cf 4f ce 02 8f 9d-9e f1 dc fb dd 9f 3e be      8..0.....>.
    0030 - 73 01 f7 78 8e c8 d0 0f-f9 bf 07 a3 c8 56 cb 8a      s..x.....V..
    0040 - f5 02 3b 97 3c c7 7c ed-13 8c 55 87 0a 4c 28 1e      ..;<.|...U..L(.
    0050 - 0e d1 ea 6f a2 78 ec 34-fc e9 91 51 5c 42 40 28      ...o.x.4...Q\B@(.
    0060 - 0c 33 2e 20 50 63 24 fd-17 18 6c a7 32 78 74 b9      .3. Pc$....l.2xt.
    0070 - 66 76 f4 63 09 1a e2 e2-64 a9 3a d6 58 7e e8 d2      fv.c....d...X~..
    0080 - bb 6b 1d 4f fc 5e a5 73-9f 22 86 f8 bc 78 43 83      .k.0.^.s."...xC.
    0090 - 44 f3 cb 7d 13 7d b5 cb-d1 3a 32 bb 78 9a b7 85      D..}.}....2.x...
    00a0 - a8 eb a4 b9 13 ea 2d 4e-ab ea 6a 0b d8 bf 88 7c      .....-N..j....|
    00b0 - 66 65 3e 4b 11 97 07 c1-c7 03 55 43 c4 21 1b a1      fe>K.....UC.!..
    00c0 - 7d 97 8e 8a 48 32 ef 20-ad b0 5e 4c 47 c1 94 50      }...H2. ...^LG..P

    Start Time: 1702035941
    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.maabedelhay.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN bWFhYmVkZWxoYXkAbWFhYmVkZWxoYXkAMTIzNDU2
235 2.7.0 Authentication successful
```

Я научился настраивать SMTP-сервер с точки зрения настроек аутентификации.

Спасибо За Внимание