Лабораторная работа № 10. Расширенные настройки SMTP-сервера

Сущенко Алина
НПИбд-01-23

Российский университет дружбы народов имени Патриса Лумумбы

2025

Цель работы

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

Настройка LMTP в Dovecot

1. На виртуальной машине `server` вошли под пользователем и открыли терминал. Перешли в режим суперпользователя:

   ```
   sudo -i
   ```

2. В дополнительном терминале запустили мониторинг работы почтовой службы:

   ```
   sudo -i
   tail -f /var/log/maillog
   ```

Настройка LMTP в Dovecot

3. Добавили в список протоколов, с которыми может работать Dovecot, протокол LMTP:

```
protocols = imap pop3 lmtp
```

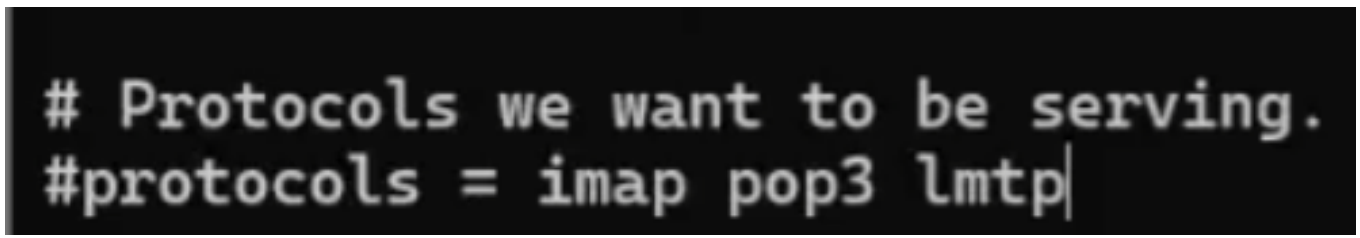


Рис.: Обновление списка разрешенных протоколов в Dovecot.

Настройка LMTP в Dovecot

4. Настроили в Dovecot сервис `lmtp` для связи с Postfix:

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

Рис.: Настройки сервера `lmtp`.

Настройка LMTP в Dovecot

5. Переопределили в Postfix передачу сообщений через unix-сокет:

   `postconf -e 'mailbox_transport = lmtp:unix:private/dovec`

6. Задали формат имени пользователя для аутентификации:

   `auth_username_format = %Ln`

```
# Username formatting before it's looked up from databases. You can use
# the standard variables here, eg. %Lu would lowercase the username, %n would
# drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
# "-AT-". This translation is done after auth_username_translation changes.
#auth_username_format = %Ln
```

Рис.: Задание формата имени пользователя для аутентификации.

Настройка LMTP в Dovecot

7. Перезапустили Postfix и Dovecot:

```
systemctl restart postfix
systemctl restart dovecot
```

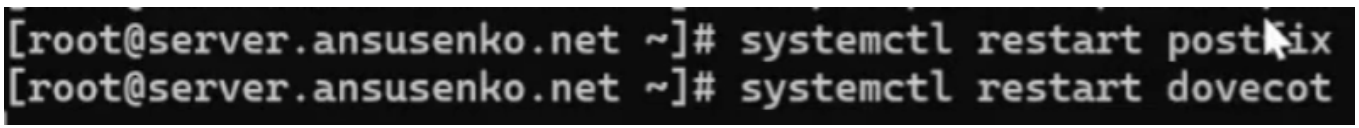


Рис.: Перезагрузка Postfix и Dovecot.

Настройка LMTP в Dovecot

8. Отправили тестовое письмо:

   ```
   echo .| mail -s "LMTP test" ansusenko@ansusenko.net
   ```

9. Просмотрели почтовый ящик пользователя:

   ```
   MAIL=~/Maildir/ mail
   ```

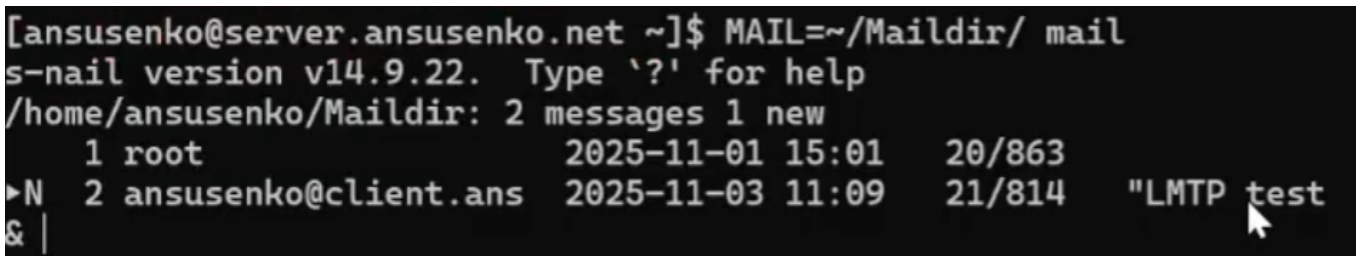


Рис.: Просмотр доставленного письма через утилиту `mail`.

Настройка LMTP в Dovecot

```
s=0/0.02/0/0, dsn=5.4.4, status=bounced (Host or domain name not found. Name service error for name=client.ansusenko.net
 type=A: Host not found)
Nov  3 11:02:58 server postfix/qmgr[8994]: 468F58B4B: removed
Nov  3 11:05:27 server dovecot[9002]: master: Warning: Killed with signal 15 (by pid=9120 uid=0 code=kill)
Nov  3 11:05:28 server dovecot[9129]: master: Dovecot v2.3.16 (7e2e900c1a) starting up for imap, pop3, lmtp (core dumps
disabled)
Nov  3 11:09:02 server postfix/postfix-script[9166]: stopping the Postfix mail system
Nov  3 11:09:02 server postfix/master[8991]: terminating on signal 15
Nov  3 11:09:03 server postfix/postfix-script[9243]: starting the Postfix mail system
Nov  3 11:09:03 server postfix/master[9245]: daemon started -- version 3.5.25, configuration /etc/postfix
Nov  3 11:09:06 server dovecot[9129]: master: Warning: Killed with signal 15 (by pid=9266 uid=0 code=kill)
Nov  3 11:09:07 server dovecot[9131]: log(9131): Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Nov  3 11:09:07 server dovecot[9276]: master: Dovecot v2.3.16 (7e2e900c1a) starting up for imap, pop3, lmtp (core dumps
disabled)
Nov  3 11:09:24 server postfix/smtpd[9280]: connect from unknown[192.168.1.30]
Nov  3 11:09:24 server postfix/smtpd[9280]: 1D3868B43: client=unknown[192.168.1.30]
Nov  3 11:09:24 server postfix/cleanup[9284]: 1D3868B43: message-id=<20251103110923.E7E428A5@client.ansusenko.net>
Nov  3 11:09:24 server postfix/qmgr[9248]: 1D3868B43: from=<ansusenko@client.ansusenko.net>, size=530, nrcpt=1 (queue ac
tive)
Nov  3 11:09:24 server postfix/smtpd[9280]: disconnect from unknown[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1
 quit=1 commands=7
Nov  3 11:09:24 server dovecot[9278]: lmtp(9287): Connect from local
Nov  3 11:09:24 server dovecot[9278]: lmtp(ansusenko)<9287><2dQ7DmSNCGlHJAAAEuOVkQ>: msgid=<20251103110923.E7E428A5@clie
nt.ansusenko.net>: saved mail to INBOX
Nov  3 11:09:24 server postfix/lmtp[9286]: 1D3868B43: to=<ansusenko@ansusenko.net>, relay=server.ansusenko.net[private/d
ovecot-lmtp], delay=0.22, delays=0.04/0.03/0.08/0.08, dsn=2.0.0, status=sent (250 2.0.0 <ansusenko@ansusenko.net> 2dQ7Dm
SNCGlHJAAAEuOVkQ Saved)
Nov  3 11:09:24 server postfix/qmgr[9248]: 1D3868B43: removed
Nov  3 11:09:24 server dovecot[9278]: lmtp(9287): Disconnect from local: Logged out (state=READY)
```

Рис.: Просмотр логов при отправке письма.

Настройка SMTP-аутентификации

1. Определили службу аутентификации пользователей:

```
service auth {
  unix_listener /var/spool/postfix/private/auth {
    group = postfix
    user = postfix
    mode = 0660
  }
  unix_listener auth-userdb {
    mode = 0600
    user = dovecot
  }
}
```

```
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
```

Настройка SMTP-аутентификации

2. Задали тип аутентификации SASL для Postfix:

```
postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'
```

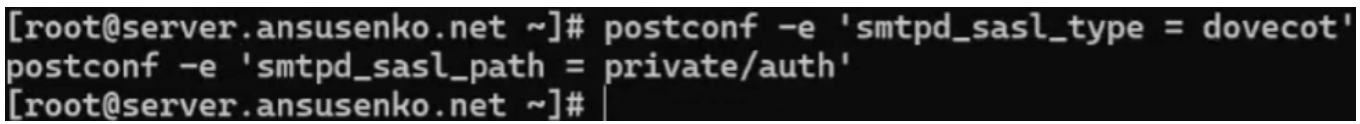


Рис.: Настройка типа аутентификации SASL для `smtpd`.

Настройка SMTP-аутентификации

3. Настроили Postfix для защиты от спамрассылок:

```
postconf -e 'smtpd_recipient_restrictions = reject_unkno
```

```
[root@server.ansusenko.net ~]# postconf -e 'smtpd_recipient_restrictions = reject_unkno
wn_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destin
ation, reject_unverified_recipient, permit'
[root@server.ansusenko.net ~]#
```

Рис.: Настройка Postfix для запрета спамрассылок.

Настройка SMTP-аутентификации

4. Ограничили приём почты только локальным адресом:

   `postconf -e 'mynetworks = 127.0.0.0/8'`

Рис.: Ограничение приема почты только локальным адресом.

Настройка SMTP-аутентификации

5. Настроили SMTP-сервер с возможностью аутентификации:

```
smtp inet n - n - - smtpd
-o smtpd_sasl_auth_enable=yes
-o smtpd_recipient_restrictions=reject_non_fqdn_recipier
```

Настройка SMTP-аутентификации

6. Перезапустили Postfix и Dovecot:

```
systemctl restart postfix
systemctl restart dovecot
```

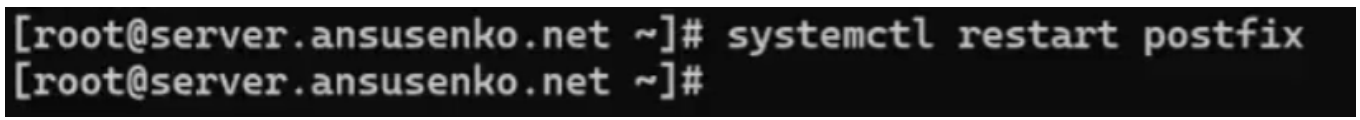


Рис.: Перезагрузка Postfix и Dovecot.

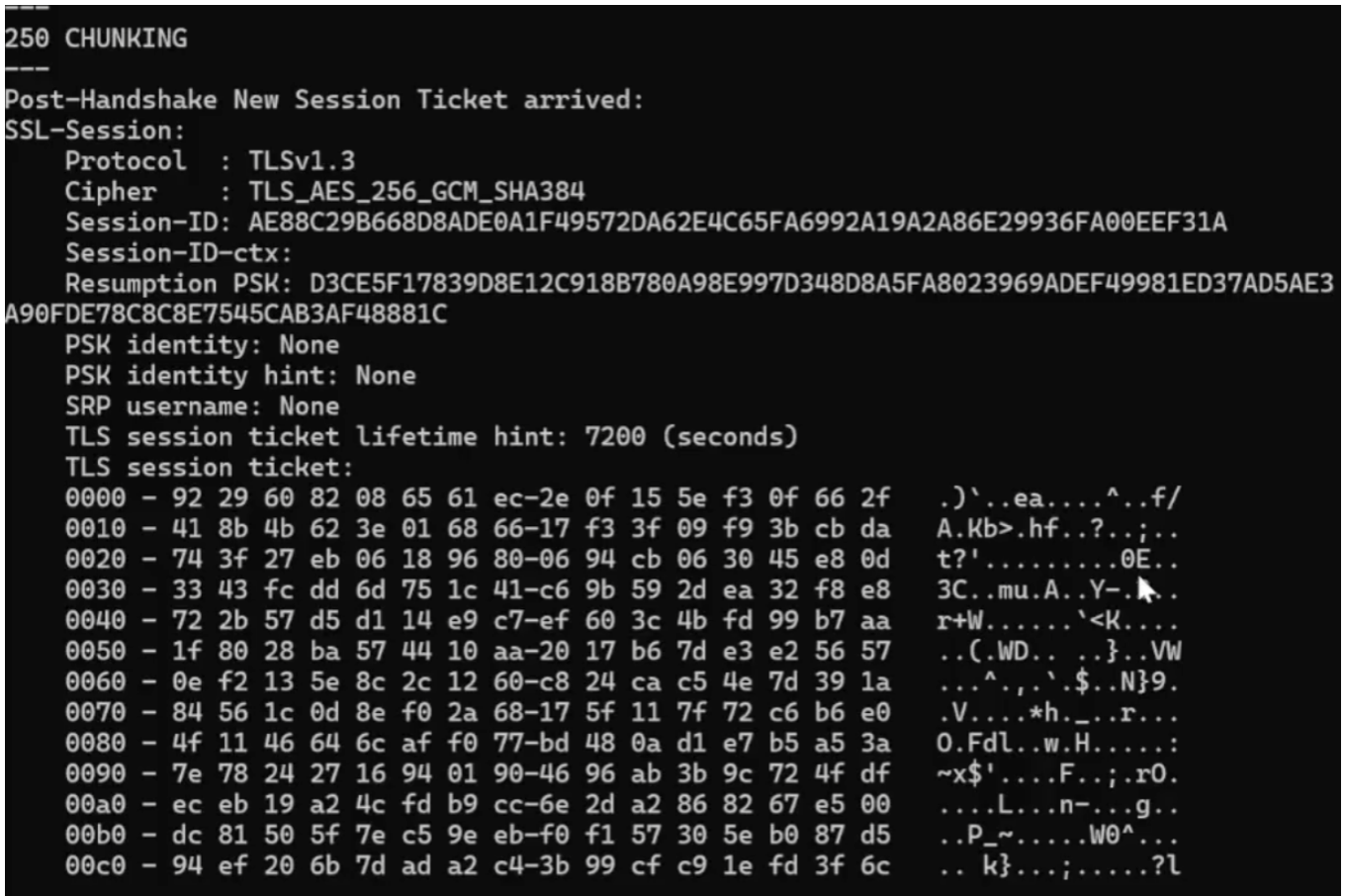
Настройка SMTP-аутентификации

7. Установили telnet на клиенте:

   ```
   sudo -i
   dnf -y install telnet
   ```

8. Протестировали соединение:

   ```
   EHLO test
   AUTH PLAIN <строка для аутентификации>
   ```



Настройка SMTP over TLS

На Alpine выполним подключение по порту, отправим себе письм

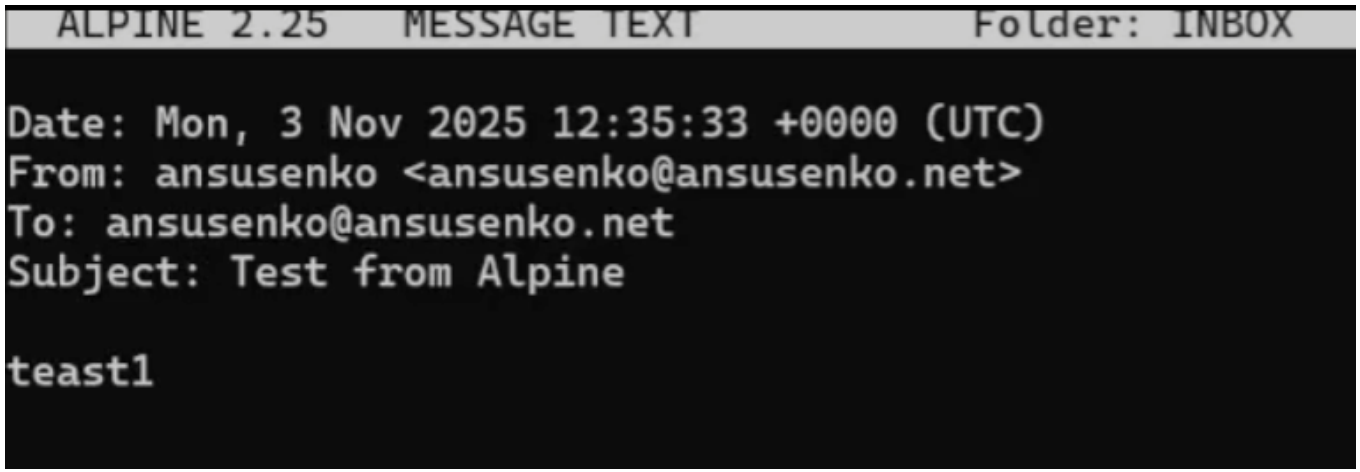


Рис.: Отправка сообщения `telnet`.

Внесение изменений в настройки внутреннего окружения

1. Скопировали конфигурационные файлы:

```
cd /vagrant/provision/server
cp -R /etc/dovecot/dovecot.conf /vagrant/provision/serve
cp -R /etc/dovecot/conf.d/10-master.conf /vagrant/provis
cp -R /etc/dovecot/conf.d/10-auth.conf /vagrant/provisio
mkdir -p /vagrant/provision/server/mail/etc/postfix/
cp -R /etc/postfix/master.cf /vagrant/provision/server/m
```

Выводы

- В результате выполнения лабораторной работы приобрели практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.
- Освоили настройку LMTP в Dovecot для интеграции с Postfix.
- Настроили SMTP-аутентификацию с использованием SASL.
- Реализовали защиту почтового сервера от использования в качестве открытого релея.
- Настроили работу SMTP over TLS для безопасной передачи почты.

Контрольные вопросы

1. Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.

- Для указания формата логина с доменом используется параметр:

  `auth_username_format = %Lu`

- Альтернативный вариант - указание полного формата:

  `auth_username_format = %n`

Контрольные вопросы

2. Какие функции выполняет почтовый Relay-сервер?

- **Пересылка почты** - передача сообщений между разными почтовыми серверами
- **Кэширование** - временное хранение сообщений при проблемах с доставкой
- **Балансировка нагрузки** - распределение почтового трафика
- **Фильтрация** - проверка почты на спам и вирусы
- **Анонимизация** - скрытие реального источника отправки почты

Контрольные вопросы

3. Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?

- **Спам-рассылки** - использование сервера для массовой рассылки спама
- **Черные списки** - IP-адрес сервера может быть внесен в DNSBL
- **Перегрузка ресурсов** - большой объем несанкционированной почты
- **Компрометация репутации** - ухудшение репутации домена и IP-адреса
- **Юридические риски** - ответственность за рассылку спама

Меры защиты от угроз Relay-сервера

- **Аутентификация** - требовать аутентификацию для отправки почты
- **Ограничение сетей** - настройка `mynetworks` только для доверенных сетей
- **Проверка получателей** - использование `smtpd_recipient_restrictions`
- **Шифрование** - обязательное использование TLS для передачи почты
- **Мониторинг** - регулярный анализ логов почтовой активности
- **Ограничение квот** - установка лимитов на объем отправляемой почты