Лабораторная работа № 10

Расширенные настройки SMTP-сервера

Беличева Дарья Михайловна

Содержание

# 1 Цель работы

Приобрести практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

# 2 Задание

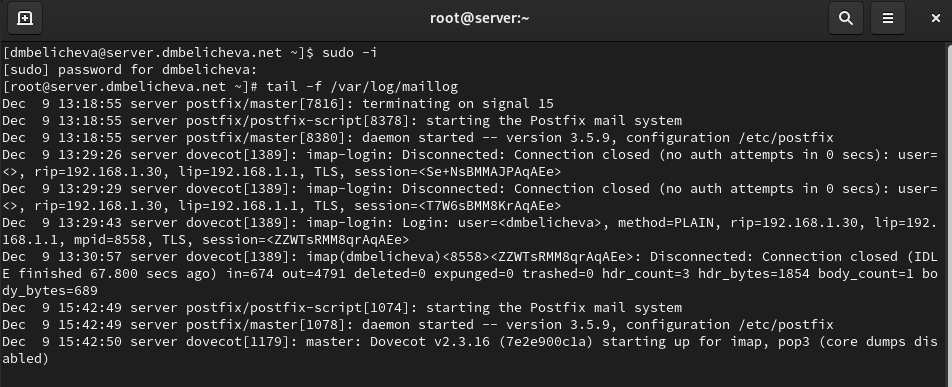
1. Настроить Dovecot для работы с LMTP.
2. Настроить аутентификацию посредством SASL на SMTP-сервере.
3. Настроить работу SMTP-сервера поверх TLS.
4. Скорректировать скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server.

# 3 Выполнение лабораторной работы

## 3.1 Настройка LMTP в Dovecote

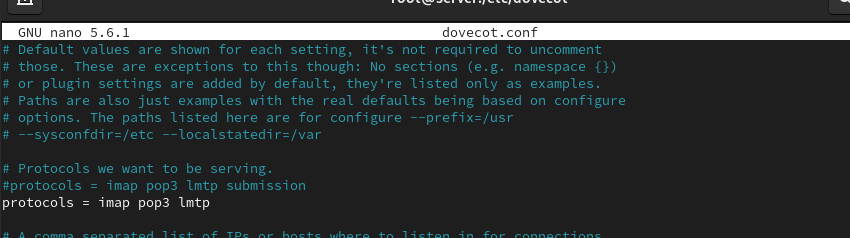
На виртуальной машине server войдем под своим пользователем и откроем терминал. Перейдем в режим суперпользователя: sudo -i

В дополнительном терминале запустим мониторинг работы почтовой службы: tail -f /var/log/maillog



Мониторинг работы почтовой службы

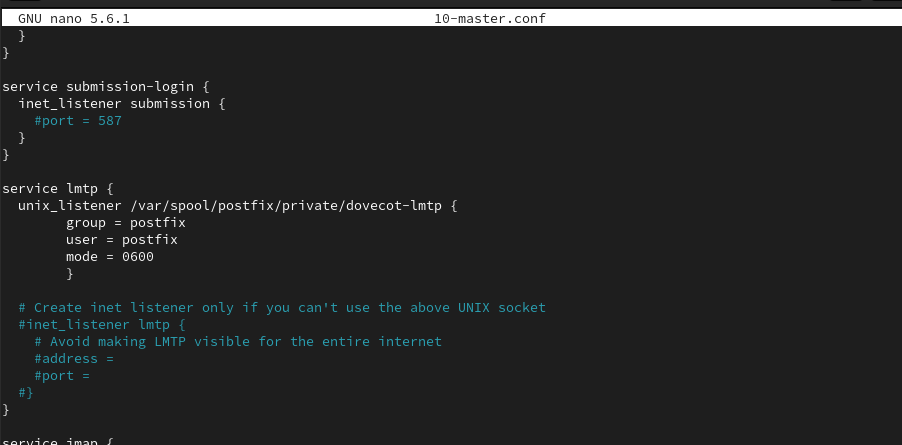
Добавим в список протоколов, с которыми может работать Dovecot, протокол LMTP. Для этого в файле /etc/dovecot/dovecot.conf укажем protocols = imap pop3 lmtp



Редактирование файла

Настроим в Dovecot сервис lmtp для связи с Postfix. Для этого в файле /etc/dovecot/conf.d/10-master.conf заменим определение сервиса lmtp на следующую запись:

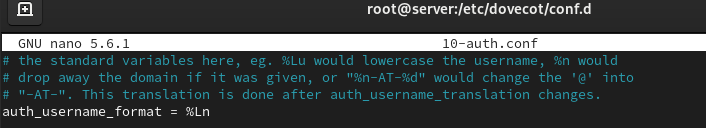
service lmtp {  
unix\_listener /var/spool/postfix/private/dovecot-lmtp {  
group = postfix  
user = postfix  
mode = 0600  
}  
}



Редактирование файла

Переопределим в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокет: postconf -e 'mailbox\_transport = lmtp:unix:private/dovecot-lmtp'

В файле /etc/dovecot/conf.d/10-auth.conf зададим формат имени пользователя для аутентификации в форме логина пользователя без указания домена: auth\_username\_format = %Ln



Редактирование файла

Перезапустим Postfix и Dovecot.

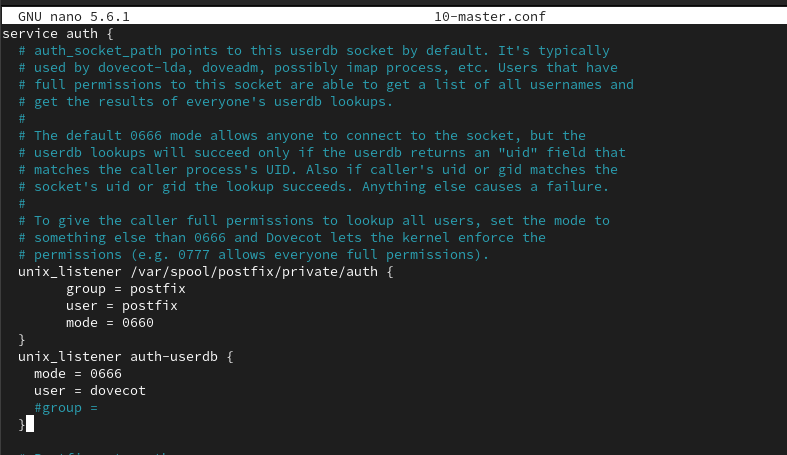
Из-под учётной записи своего пользователя отправим письмо с клиента: echo .| mail -s "LMTP test" dmbelicheva@dmbelicheva.net

На сервере просмотрим почтовый ящик пользователя: MAIL=~/Maildir/ mail

Там оказалось пусто, потому что письмо не было доставлено в связи с какими-то проблемами.

## 3.2 Настройка SMTP-аутентификации

В файле /etc/dovecot/conf.d/10-master.conf определим службу аутентификации пользователей:



Редактирование файла

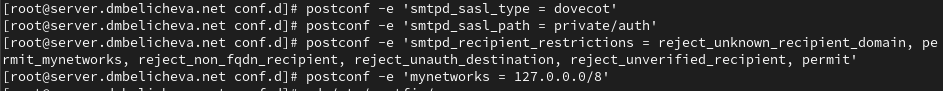
Для Postfix зададим тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету:

postconf -e 'smtpd\_sasl\_type = dovecot'  
postconf -e 'smtpd\_sasl\_path = private/auth'

Настроим Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины (имеется в виду локальных пользователей сервера), обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок (порядок указания опций имеет значение):

postconf -e 'smtpd\_recipient\_restrictions =  
reject\_unknown\_recipient\_domain,  
permit\_mynetworks, reject\_non\_fqdn\_recipient,   
reject\_unauth\_destination,reject\_unverified\_recipient, permit'

В настройках Postfix ограничем приём почты только локальным адресом SMTP-сервера сети: postconf -e 'mynetworks = 127.0.0.0/8'



Команды postconf

Для проверки работы аутентификации временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Для этого необходимо в файле /etc/postfix/master.cf изменим строки



Редактирование файла

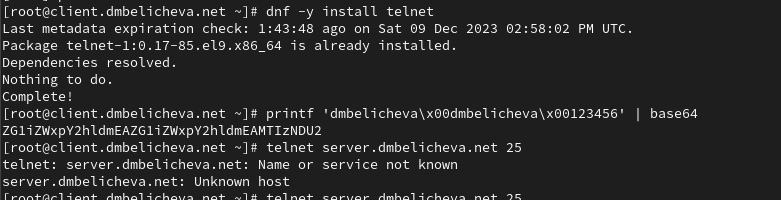
Перезапустим Postfix и Dovecot:

systemctl restart postfix  
systemctl restart dovecot

На клиенте установим telnet: dnf -y install telnet

На клиенте получим строку для аутентификации, вместо username указав логин вашего пользователя, а вместо password указав пароль этого пользователя: printf 'username\x00username\x00password' | base64

Подключимся на клиенте к SMTP-серверу посредством telnet: telnet server.dmbelicheva.net 25



Получение строки для аутентификации и подключение через telnet

Подключение не удалось.

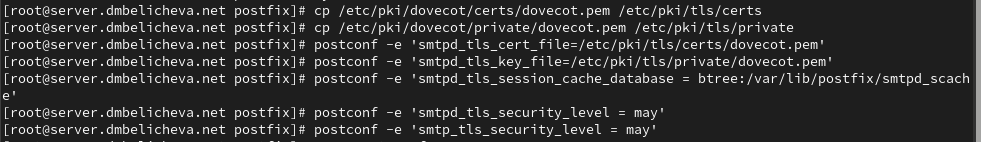
## 3.3 Настройка SMTP over TLS

Настроим на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно скопируем необходимые файлы сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги (чтобы не было проблем с SELinux):

cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs  
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private

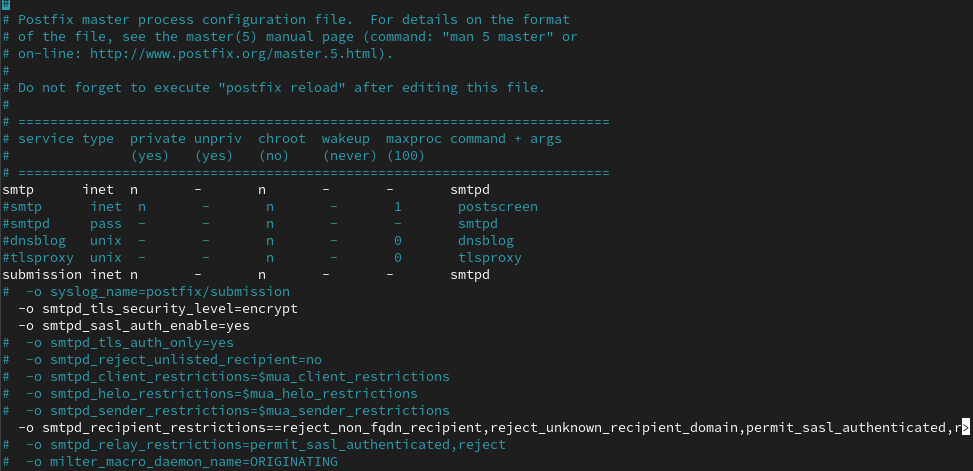
Сконфигурируем Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности:

postconf -e 'smtpd\_tls\_cert\_file=/etc/pki/tls/certs/dovecot.pem'  
postconf -e 'smtpd\_tls\_key\_file=/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'



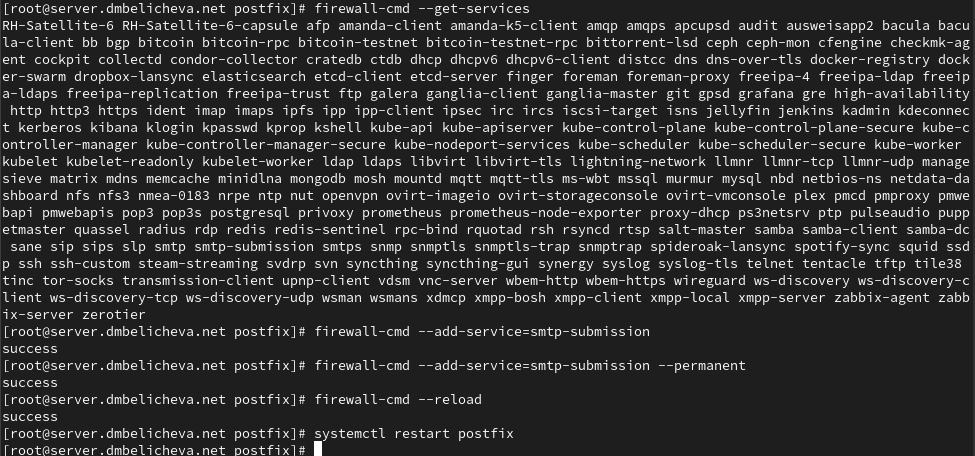
Настройка SMTP over TLS

Для того чтобы запустить SMTP-сервер на 587-м порту, в файле /etc/postfix/master.cf изменим строки



Редактирование файла

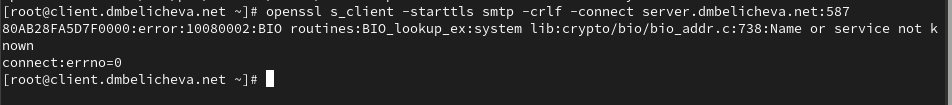
Настроим межсетевой экран, разрешив работать службе smtp-submission:



Настройка межсетевого экрана

Перезапустим Postfix: systemctl restart postfix

На клиенте подключимся к SMTP-серверу через 587-й порт посредством openssl: openssl s\_client -starttls smtp -crlf -connect server.dmbelicheva.net:587

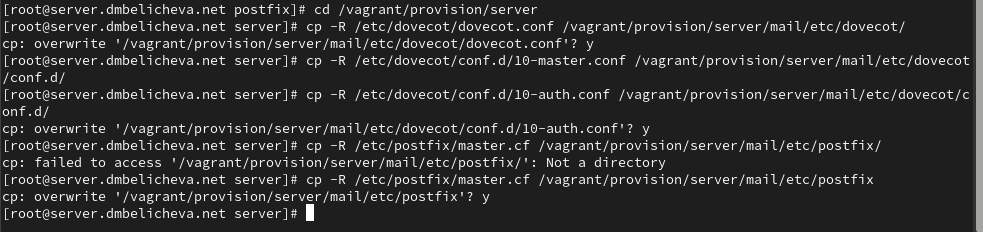


openssl

Подключение не удалось.

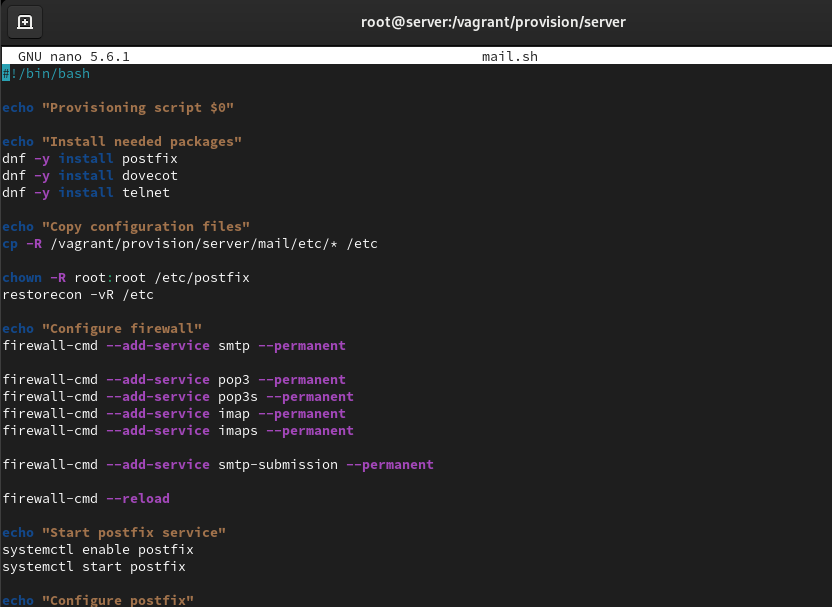
## 3.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/. В соответствующие подкаталоги поместим конфигурационные файлы Dovecot и Postfix:



Внесение изменений в настройки внутреннего окружения виртуальной машины

Внесем соответствующие изменения по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh:



Редактирование файла

Внесем изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet.



Редактирование файла

# 4 Выводы

В процессе выполнения данной лабораторной работы я приобрела практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

# 5 Контрольные вопросы

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

auth\_username\_format = %Lu%d

1. Какие функции выполняет почтовый Relay-сервер?

обеспечивает приём сообщения, временное хранение (часто не больше нескольких минут в случае мгновенных сообщений, до недели в случае электронной почты), пересылку сообщения узлу-получателю (или следующему релею)

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

спам, перехват и изменение электронных сообщений.