

Лабораторная работа №10

Расширенные настройки SMTP-сервера

Газизянов Владислав Альбертович

2025-12-19

Содержание I

1. Цели и задачи

Цель: Приобретение навыков расширенной настройки SMTP-сервера.

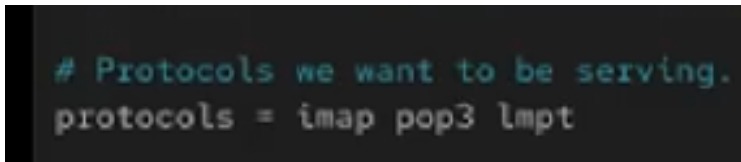
Задачи: - Настроить Dovecot для работы с протоколом LMTP - Реализовать SMTP-аутентификацию через SASL - Настроить работу SMTP поверх TLS - Автоматизировать настройку через скрипт Vagrant

```
[vagazizianov@server.vagazizianov.net ~]$ sudo -i
[sudo] password for vagazizianov:
[root@server.vagazizianov.net ~]# tail -f /var/log/maillog
Oct 30 17:33:25 server postfix/smtpd[18849]: disconnect from unknown[192.168.1.30] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
Oct 30 17:33:25 server postfix/local[18864]: D5F9F4985F: to=<vagazizianov@vagazizianov.net>, relay=local, delay=0.49, delays=0.28/0.04/0.0.17, dsn=2.0.0, status=sent (delivered to maildir)
Oct 30 17:33:25 server postfix/qmgr[12426]: D5F9F4985F: removed
Oct 30 17:38:26 server dovecot[12607]: pop3-login: Login: user=<vagazizianov>, method=PLAIN, rip=192.168.1.1, lip=192.168.1.1, mpid=19549, secured, session=<V6Jmt2NCSobAqAEB>
Oct 30 17:39:26 server dovecot[12607]: pop3(vagazizianov)<19549><V6Jmt2NCSobAqAEB>: Disconnected: Logged out top=0/0, retr=1/717, del=1/2, size=1402
Oct 30 17:54:27 server dovecot[12607]: imap(vagazizianov)<18652><71MYm2NCAuPAqAEe>: Disconnected: Connection closed (IDLE finished 246.314 secs ago) in=755 out=4443 deleted=0 expunged=0 trashed=0 hdr_count=2 hdr_bytes=1388 body_count=0 body_bytes=0
Oct 30 17:54:27 server dovecot[12607]: imap(vagazizianov)<18509><7ptjlmNC2MPAqAEe>: Disconnected: Connection closed (IDLE finished 3.326 secs ago) in=3634 out=11202 deleted=0 expunged=0 trashed=0 hdr_count=2 hdr_bytes=1388 body_count=1 body_bytes=701
Nov 14 14:16:35 server dovecot[1508]: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3
Nov 14 14:16:40 server postfix/postfix-script[1943]: starting the Postfix mail system
Nov 14 14:16:41 server postfix/master[1953]: daemon started -- version 3.8.5, configuration /etc/postfix
```

Рисунок 1: Запуск мониторинга и настройка LMTP в Dovecot

2. Настройка LMTP в Dovecot

Конфигурация протокола доставки: - Добавление LMTP в поддерживаемые протоколы - Настройка сервиса LMTP для взаимодействия с Postfix - Интеграция через Unix-сокеты

A screenshot of a terminal window showing a configuration file. The text is in a light blue/cyan color on a dark background. It shows a comment line followed by a line that sets the 'protocols' variable to include 'imap', 'pop3', and 'lmtp'.

```
# Protocols we want to be serving.  
protocols = imap pop3 lmtp
```

Рисунок 2: Настройка LMTP-транспорта в Postfix и перезапуск служб

3. Тестирование LMTP

Проверка работоспособности: - Перезапуск служб Postfix и Dovecot - Отправка тестового письма с клиента - Проверка доставки в почтовый ящик

```
[root@server.vagazizianov.net ~]# nano /etc/dovecot/conf.d/10-master.conf  
[root@server.vagazizianov.net ~]# postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'  
[root@server.vagazizianov.net ~]# nano
```

Рисунок 3: Тестирование отправки письма через LMTP

4. Настройка SMTP-аутентификации

Конфигурация SASL: - Настройка службы аутентификации в Dovecot -
Конфигурация параметров SASL в Postfix - Определение ограничений получателей

```
[root@server.vagazizianov.net ~]# nano /etc/dovecot/conf.d/10  
[root@server.vagazizianov.net ~]# systemctl restart postfix  
[root@server.vagazizianov.net ~]# systemctl restart dovecot
```

Рисунок 4: Настройка службы аутентификации SASL и параметров Postfix

5. Мастер-конфигурация Postfix

Включение аутентификации: - Изменение файла master.cf - Поддержка SASL на порту 25 - Настройка ограничений доступа

```
GNU nano 8.1 /etc/dovecot/conf.d/10-master.conf
#process_limit = 1024
}

service pop3 {
  # Max. number of POP3 processes (connections)
  #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
  }
  unix_listener auth-userdb {
    mode = 0660
    user = dovecot
  }
}

service auth-worker {
  # Auth worker process is run as root by default, so that it can access
  # /etc/shadow. If this isn't necessary, the user should be changed to
  # $default_internal_user.
  #user = root
}
```

6. Тестирование аутентификации

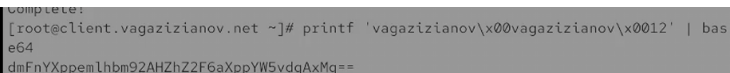
Проверка механизма PLAIN: - Генерация строки аутентификации в base64 -
Подключение через telnet к порту 25 - Успешная проверка учетных данных

```
[root@server.vagazizianov.net ~]# postconf -e 'smtpd_sasl_type = dovecot'  
[root@server.vagazizianov.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
```

Рисунок 6: Генерация строки аутентификации и тестирование через telnet

7. Настройка TLS

Подготовка шифрования: - Копирование сертификатов из Dovecot - Настройка параметров TLS в Postfix - Конфигурация путей к сертификатам

A terminal window with a dark background. The prompt is [root@client.vagazizianov.net ~]#. The command is printf 'vagazizianov\x00vagazizianov\x0012' | base64. The output is dmFnYXppemlhbW92AHZhZ2F6aXppYW5vdgAxMg==.

```
Complete:  
[root@client.vagazizianov.net ~]# printf 'vagazizianov\x00vagazizianov\x0012' | bas  
e64  
dmFnYXppemlhbW92AHZhZ2F6aXppYW5vdgAxMg==
```

Рисунок 7: Копирование сертификатов и настройка TLS в Postfix

8. Конфигурация порта submission

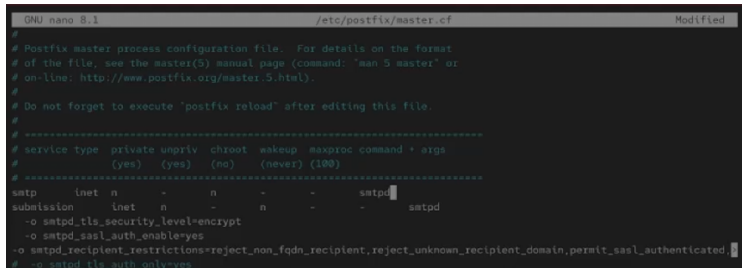
Настройка защищенного доступа: - Запуск сервиса на порту 587 - Поддержка STARTTLS - Обязательная аутентификация - Правила межсетевого экрана

```
[root@server.vagazizianov.net ~]# systemctl restart postfix
[root@server.vagazizianov.net ~]# systemctl restart dovecot
[root@server.vagazizianov.net ~]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
[root@server.vagazizianov.net ~]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
[root@server.vagazizianov.net ~]# postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
[root@server.vagazizianov.net ~]# postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
[root@server.vagazizianov.net ~]# postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
[root@server.vagazizianov.net ~]# postconf -e 'smtpd_tls_security_level = may'
[root@server.vagazizianov.net ~]# postconf -e 'smtp_tls_security_level = may'
[root@server.vagazizianov.net ~]#
```

Рисунок 8: Настройка порта 587 с TLS и правил FirewallD

9. Тестирование TLS

Проверка шифрования: - Подключение через openssl - Проверка поддержки STARTTLS - Аутентификация в зашифрованном канале



```
GNU nano 8.1 /etc/postfix/master.cf Modified
#
# 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
submission inet  n       -       n       -       -       smtpd
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated
  -o smtpd_tls_auth_only=yes
```

Рисунок 9: Тестирование TLS-подключения через openssl

10. Настройка почтового клиента

Интеграция с Evolution: - Настройка порта 587 - Включение STARTTLS - Конфигурация учётной записи

```

Early data was not sent
Verify return code: 18 (self-signed certificate)
---
250 CHUNKING
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol : TLSv1.3
    Cipher   : TLS_AES_256_GCM_SHA384
    Session-ID: 89DDE8DE4D65318F00BC1FB4A2AA10F3B47F4E25C4177CFEE9A352EAE40EBA99
    Session-ID-ctx:
    Resumption PSK: 5368A163C29BEFE4869667C82718B9B08C5E4AC21C831FF4C80AB5138C67374
A36830B70342E0D25FF7B29EC4CD0F65E
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
0000 - 3e 82 78 bc 59 b6 63 e8-37 d4 33 6d 36 1b 6b 81  >.x.Y.c.7.3m6.k.
0010 - e2 89 16 30 ac 77 d0 2f-61 4a 2a 1f fe 4c 7a 79  ...0.w./aJ*.Lzy
0020 - 95 eb 58 3e c2 35 a2 1e-3a d1 c0 14 0a 57 9d 66  ..X>.S.....W.f
0030 - 73 42 54 19 45 59 ea 17-c1 3d 1c be 75 71 40 af  sBT.EY...=..uq@.
0040 - ad a9 2e de 0b 89 29 ba-1d 1c e0 92 e1 f1 18 e1  .....).....
0050 - e5 4c 1a 87 be bf 06 51-1d 0f 3e 50 d6 fa 6d 03  .L.....Q..>P..m.
0060 - 2e 53 ed 23 6f 61 89 c1-2e ad 4a 8d 60 6d 9b 40  .S.#oa....J.'m.@
0070 - ab 9f 50 b3 8e 2c 52 91-f4 4f 77 86 b2 0d 47 7f  ..P...R..Ow...G.
0080 - 58 a6 47 9a 00 62 0c 92-54 c7 42 50 39 05 d2 bf  X.G..b..T.BP9...
0090 - e9 55 a3 e5 c5 52 9a ca-a5 a2 f3 c8 f5 0d 2a 85  .U...R.....*.
00a0 - 4c 4f eb 6d 06 1d 9d 0a-62 4a ca cb e6 d0 0d c0  L0.m....bJ.....
00b0 - 52 51 1b f6 c8 83 7d 03-7f 65 26 c8 17 37 0d 2d  03..1..f.....

```

11. Контрольные вопросы

Основные вопросы: - **Формат аутентификации с доменом:**

`auth_username_format = %Ln` - **Функции Relay-сервера:** Пересылка между системами, фильтрация, кэширование - **Угрозы открытого ретранслятора:**

Спам-рассылки, перегрузка, блокировка IP

12. Выводы

Результаты работы: - Настроен протокол LMTP для локальной доставки почты -
Реализована аутентификация SMTP через SASL - Настроено шифрование через TLS
на порту 587 - Создан автоматизированный сценарий развертывания -
Приобретены навыки расширенной настройки почтовых серверов