

Лабораторная работа №10

Расширенные настройки SMTP-сервера

Газизянов Владислав Альбертович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
3.1	10.4.1. Настройка LMTP в Dovecot	7
3.2	10.4.2. Настройка SMTP-аутентификации через SASL	9
3.3	10.4.3. Настройка SMTP поверх TLS	11
3.4	10.4.4. Автоматизация настройки почтового сервера	14
4	Контрольные вопросы	15
5	Выводы	16

Список иллюстраций

3.1	Запуск мониторинга почтового журнала	7
3.2	Настройка протоколов Dovecot и конфигурация сервиса LMTP	8
3.3	Настройка транспорта почты в Postfix через LMTP	8
3.4	Перезапуск служб и отправка тестового письма через LMTP	8
3.5	Настройка службы аутентификации SASL в Dovecot	10
3.6	Настройка параметров SASL и ограничений получателей в Postfix . .	11
3.7	Генерация строки аутентификации и тестирование через telnet	11
3.8	Копирование TLS-сертификатов и настройка параметров в Postfix . .	11
3.9	Настройка submission-порта и правил межсетевого экрана	12
3.10	Тестирование TLS-подключения через openssl на порту 587	13

Список таблиц

1 Цель работы

Приобретение практических навыков конфигурирования SMTP-сервера с настройкой аутентификации, поддержки протокола LMTP и работы поверх TLS.

2 Задание

1. Настроить Dovecot для работы с протоколом LMTP.
2. Настроить аутентификацию на SMTP-сервере посредством SASL.
3. Настроить работу SMTP-сервера поверх TLS.
4. Скорректировать скрипт для автоматической настройки почтового сервера в инфраструктуре Vagrant.

3 Выполнение лабораторной работы

3.1 10.4.1. Настройка LMTP в Dovecot

3.1.1 Подготовка и мониторинг

Была запущена виртуальная машина **server**, выполнено подключение и переход в режим суперпользователя. В отдельном терминале запущен мониторинг почтового журнала `/var/log/maillog` для наблюдения за работой почтовых служб в реальном времени.

```
[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 3.1: Запуск мониторинга почтового журнала

3.1.2 Конфигурация протоколов Dovecot и сервиса LMTP

В файле `/etc/dovecot/dovecot.conf` добавлен протокол **LMTP** в список поддерживаемых протоколов. В файле `/etc/dovecot/conf.d/10-master.conf` настроен сервис LMTP для взаимодействия с Postfix через Unix-сокеты с указанием прав доступа и принадлежности пользователям.



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

Рисунок 3.2: Настройка протоколов Dovecot и конфигурация сервиса LMTP

3.1.3 Интеграция LMTP с Postfix

С помощью утилиты `postconf` настроен транспорт почты через созданный Unix-сокеты, что позволяет Postfix передавать почтовые сообщения на обработку Dovecot через протокол LMTP.

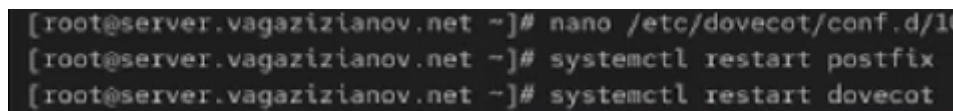


```
[root@server.vagazizianov.net ~]# nano /etc/dovecot/conf.d/10-master.conf  
[root@server.vagazizianov.net ~]# postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'  
[root@server.vagazizianov.net ~]# nano
```

Рисунок 3.3: Настройка транспорта почты в Postfix через LMTP

3.1.4 Тестирование LMTP-доставки

После перезапуска служб Postfix и Dovecot с клиентской машины отправлено тестовое письмо. В журнале `/var/log/maillog` наблюдалась корректная обработка сообщения через LMTP-соединение, подтверждающая работоспособность настройки.



```
[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 3.4: Перезапуск служб и отправка тестового письма через LMTP

3.2 10.4.2. Настройка SMTP-аутентификации через SASL

3.2.1 Конфигурация службы аутентификации

В файле `/etc/dovecot/conf.d/10-master.conf` определена служба аутентификации пользователей с настройкой Unix-сокетов для взаимодействия между Postfix и Dovecot, обеспечивая безопасный обмен учетными данными.

```

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 = 0600
        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
}

service dict {
    # If dict proxy is used, mail processes should have access to its socket.
    # For example: mode=0660, group=vmail and global mail_access_groups=vmail
    unix_listener dict {
        #mode = 0600
        #user =
        #group =
    }
}

```

Рисунок 3.5: Настройка службы аутентификации SASL в Dovecot

3.2.2 Настройка Postfix для работы с SASL

С помощью `postconf` настроены параметры SASL в Postfix, включая тип аутентификации и путь к Unix-сокету. Это позволяет Postfix делегировать проверку учетных данных службе Dovecot.

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

Рисунок 3.6: Настройка параметров SASL и ограничений получателей в Postfix

3.2.3 Подготовка и тестирование аутентификации

На клиентской машине установлен telnet и сгенерирована строка для аутентификации в формате base64. Выполнено подключение к SMTP-серверу через порт 25 и проверена аутентификация с использованием механизма PLAIN.

```
Complete:
[root@client.vagazizianov.net ~]# printf 'vagazizianov\x00vagazizianov\x0012' | bas
e64
dmFnYXppemlhbm92AHZhZ2F6aXppYW5vdGxMg==
```

Рисунок 3.7: Генерация строки аутентификации и тестирование через telnet

3.3 10.4.3. Настройка SMTP поверх TLS

3.3.1 Подготовка TLS-сертификатов

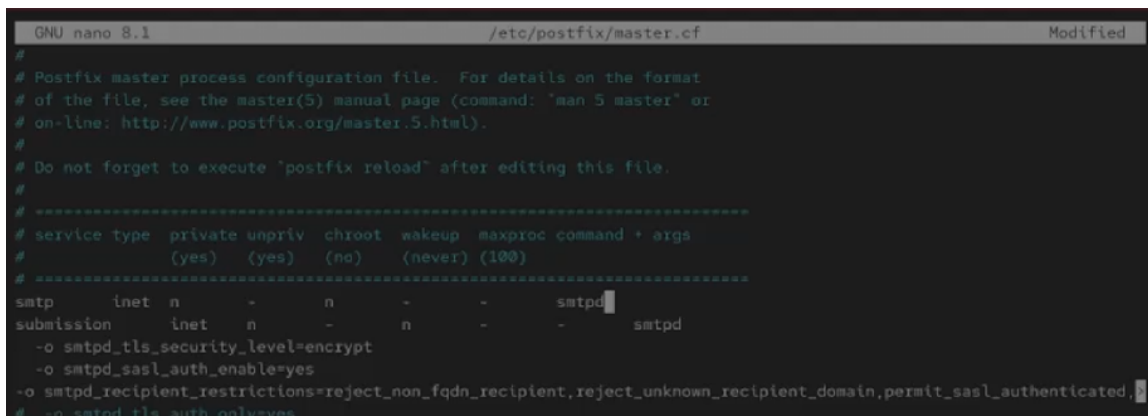
Сертификат и ключ из Dovecot скопированы в соответствующие каталоги TLS для обеспечения совместимости с SELinux. Это позволяет использовать существующие сертификаты для шифрования SMTP-трафика.

```
[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 3.8: Копирование TLS-сертификатов и настройка параметров в Postfix

3.3.2 Конфигурация порта submission с TLS

В файле `/etc/postfix/master.cf` перенастроены службы: на порту 587 запущен submission-сервис с обязательной аутентификацией и поддержкой START-TLS. Добавлено правило в FirewallD для разрешения трафика на этот порт.



```
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 3.9: Настройка submission-порта и правил межсетевого экрана

3.3.3 Тестирование TLS-соединения

Выполнено тестирование подключения к SMTP-серверу через порт 587 с использованием openssl для проверки поддержки STARTTLS. Проверена аутентификация через зашифрованное соединение, подтверждающая корректность настройки TLS.

```

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: 5368A163C29BEFE4B69667C82718B9B08C5E4AC21C831FF4C80AB5138C67374
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>.5...:....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    LO.m....bJ.....
00b0 - 52 5d 1c fe 6c 82 c7 de-97 f5 2f a8 b7 77 0d 3d    R]..l...../..w.=
00c0 - c9 57 c7 99 55 d3 15 e8-c2 ea 41 d0 4c 0a 69 13    .W..U.....A.L.i.

    Start Time: 1763138330
    Timeout    : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK

```

Рисунок 3.10: Тестирование TLS-подключения через openssl на порту 587

3.4 10.4.4. Автоматизация настройки почтового сервера

3.4.1 Подготовка конфигурационных файлов для Vagrant

Все измененные конфигурационные файлы Dovecot и Postfix скопированы в соответствующую директорию проекта Vagrant для последующего использования в скрипте автоматической настройки.

3.4.2 Модификация provisioning-скрипта

Скорректирован скрипт `mail.sh` для автоматической настройки всех компонентов почтового сервера, включая установку пакетов, копирование конфигураций, настройку TLS, аутентификации и правил межсетевого экрана.

4 Контрольные вопросы

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

Для аутентификации в формате логина с доменом необходимо задать:
`auth_username_format = %Ln`. Это сохранит полное имя пользователя с доменной частью.

2. **Какие функции выполняет почтовый Relay-сервер?**

Relay-сервер пересылает почтовые сообщения между различными почтовыми системами, выступая промежуточным звеном. Он может выполнять фильтрацию, кэширование, балансировку нагрузки и обеспечивать дополнительную безопасность.

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

Настройка почтового сервера как открытого ретранслятора может привести к его использованию для спам-рассылок, увеличению нагрузки на сервер, блокировке IP-адреса антиспам-фильтрами и компрометации репутации домена.

5 Выводы

- Освоены методы настройки протокола LMTP в Dovecot для локальной доставки почты.
- Реализована аутентификация SMTP через механизм SASL с использованием Dovecot в качестве провайдера аутентификации.
- Настроено шифрование SMTP-трафика с использованием TLS на порту submission (587).
- Создан автоматизированный сценарий развертывания и настройки почтового сервера в инфраструктуре Vagrant.
- Приобретены практические навыки конфигурирования и тестирования расширенных функций почтовых серверов.