Отчёт по лабораторной работе №10

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Содержание

# 1. Цель работы

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

# 2. Выполнение лабораторной работы

## 2.1 Настройка LMTP в Dovecote

Вход в систему выполнен под пользователем с последующим переходом в режим суперпользователя с помощью команды sudo -i, что подтверждается приглашением root@server ([рис. 1](#fig-1)). Это обеспечивает права для изменения конфигурации почтовых служб.

|  |
| --- |
| Рисунок 1: Переход в режим суперпользователя и мониторинг журнала maillog |

В дополнительном терминале запущен мониторинг журнала почтовой службы командой tail -f /var/log/maillog, что позволяет в реальном времени отслеживать события Postfix и Dovecot, включая запуск демонов и обработку соединений ([рис. 1](#fig-1)).

В конфигурационном файле /etc/dovecot/dovecot.conf в список обслуживаемых протоколов добавлен протокол LMTP посредством строки protocols = imap pop3 lmtp, что расширяет функциональность Dovecot для работы с LMTP ([рис. 2](#fig-2)).

|  |
| --- |
| Рисунок 2: Добавление протокола lmtp в конфигурации Dovecot |

В файле /etc/dovecot/conf.d/10-master.conf выполнена настройка сервиса lmtp, где определён unix-сокет /var/spool/postfix/private/dovecot-lmtp с параметрами доступа user = postfix, group = postfix, mode = 0600, обеспечивающими взаимодействие Dovecot с Postfix через локальный сокет ([рис. 3](#fig-3)).

|  |
| --- |
| Рисунок 3: Настройка сервиса lmtp и unix-сокета для взаимодействия с Postfix |

В конфигурации Postfix параметр mailbox\_transport переопределён командой postconf -e 'mailbox\_transport = lmtp:unix:private/dovecot-lmtp', что направляет доставку почты через unix-сокет Dovecot вместо прямой локальной доставки ([рис. 4](#fig-4)).

|  |
| --- |
| Рисунок 4: Переопределение mailbox\_transport в Postfix |

В файле /etc/dovecot/conf.d/10-auth.conf установлен формат имени пользователя auth\_username\_format = %Ln, что обеспечивает аутентификацию по логину без доменной части ([рис. 5](#fig-5)).

|  |
| --- |
| Рисунок 5: Настройка формата имени пользователя в Dovecot |

После внесения изменений выполнен перезапуск служб postfix и dovecot командами systemctl restart postfix и systemctl restart dovecot, что активирует обновлённые параметры конфигурации ([рис. 6](#fig-6)).

|  |
| --- |
| Рисунок 6: Перезапуск служб Postfix и Dovecot |

С клиента отправлено тестовое письмо командой echo .| mail -s "LMTP test" alkamal@alkamal.net, что инициирует передачу сообщения через SMTP на сервер ([рис. 7](#fig-8)).

|  |
| --- |
| Рисунок 7: Отправка тестового письма с клиента |

На сервере выполнена проверка почтового ящика пользователя с использованием переменной MAIL=~/Maildir/ и команды mail. В списке сообщений отображается письмо с темой «LMTP test», что подтверждает корректную доставку через LMTP в каталог Maildir ([рис. 8](#fig-9)).

|  |
| --- |
| Рисунок 8: Просмотр содержимого Maildir и подтверждение доставки письма |

## 2.2 Настройка SMTP-аутентификации

В файле /etc/dovecot/conf.d/10-master.conf определена служба аутентификации service auth, в которой задан unix-сокет /var/spool/postfix/private/auth с параметрами user = postfix, group = postfix, mode = 0660. Это обеспечивает доступ Postfix к механизму SASL-аутентификации Dovecot через локальный сокет. Дополнительно определён unix\_listener auth-userdb с правами mode = 0600 и пользователем dovecot, что ограничивает доступ к базе пользователей процессом Dovecot ([рис. 9](#fig-10)).

|  |
| --- |
| Рисунок 9: Определение службы аутентификации service auth в Dovecot |

В Postfix задан тип SASL-аутентификации dovecot и путь к unix-сокету private/auth с помощью параметров smtpd\_sasl\_type и smtpd\_sasl\_path. Это настраивает smtpd на использование Dovecot как backend-аутентификатора ([рис. 10](#fig-11)).

|  |
| --- |
| Рисунок 10: Настройка smtpd\_sasl\_type и smtpd\_sasl\_path в Postfix |

Параметр smtpd\_recipient\_restrictions настроен с последовательностью: reject\_unknown\_recipient\_domain — отклонение писем для неизвестных доменов; permit\_mynetworks — разрешение для доверенной сети; reject\_non\_fqdn\_recipient — запрет некорректных адресов; reject\_unauth\_destination — запрет релея для неразрешённых направлений; reject\_unverified\_recipient — проверка существования получателя; permit — окончательное разрешение при выполнении условий. Это предотвращает использование сервера как SMTP relay ([рис. 10](#fig-11)).

В параметре mynetworks установлено значение 127.0.0.0/8, что ограничивает приём почты только локальными соединениями ([рис. 10](#fig-11)).

В файле /etc/postfix/master.cf для сервиса smtp добавлены параметры -o smtpd\_sasl\_auth\_enable=yes и модифицированы ограничения получателей, что временно включает аутентификацию на порту 25 для тестирования ([рис. 11](#fig-12)).

|  |
| --- |
| Рисунок 11: Модификация сервиса smtp в master.cf для включения SASL |

После внесения изменений выполнен перезапуск служб postfix и dovecot, что активирует новую конфигурацию аутентификации ([рис. 12](#fig-13)).

|  |
| --- |
| Рисунок 12: Перезапуск служб Postfix и Dovecot |

На клиенте установлен пакет telnet с использованием dnf, что позволяет выполнить ручное тестирование SMTP-соединения ([рис. 13](#fig-14)).

|  |
| --- |
| Рисунок 13: Установка telnet на клиенте |

Сформирована строка аутентификации в формате base64 командой printf 'alkamal\x00alkamal\x00123456' | base64, затем выполнено подключение к SMTP-серверу по порту 25. После команды EHLO test сервер объявил поддержку AUTH PLAIN. Команда AUTH PLAIN <base64> завершилась ответом 235 2.7.0 Authentication successful, что подтверждает корректную работу SASL-аутентификации через Dovecot ([рис. 14](#fig-15)).

|  |
| --- |
| Рисунок 14: Тестирование SMTP-аутентификации через telnet |

## 2.3 Настройка SMTP over TLS

На сервере выполнено копирование временного сертификата и закрытого ключа Dovecot из каталога /etc/pki/dovecot в соответствующие подкаталоги /etc/pki/tls/certs и /etc/pki/tls/private, после чего в Postfix заданы параметры smtpd\_tls\_cert\_file, smtpd\_tls\_key\_file, smtpd\_tls\_session\_cache\_database, а также уровни безопасности smtpd\_tls\_security\_level = may и smtp\_tls\_security\_level = may, что активирует поддержку TLS для входящих и исходящих SMTP-соединений ([рис. 15](#fig-16)).

|  |
| --- |
| Рисунок 15: Настройка TLS-параметров в Postfix |

В файле /etc/postfix/master.cf оставлен стандартный сервис smtp, а также добавлен сервис submission на порту 587 с параметрами -o smtpd\_tls\_security\_level=encrypt, -o smtpd\_sasl\_auth\_enable=yes и ограничениями получателей, что обеспечивает обязательное использование TLS и аутентификации для клиентов ([рис. 16](#fig-18)).

|  |
| --- |
| Рисунок 16: Добавление сервиса submission в master.cf |

В межсетевом экране разрешена служба smtp-submission командами firewall-cmd --add-service=smtp-submission и с сохранением правила --permanent, после чего выполнена перезагрузка конфигурации брандмауэра и перезапуск Postfix ([рис. 17](#fig-19)).

|  |
| --- |
| Рисунок 17: Настройка firewall и перезапуск Postfix |

С клиента выполнено подключение к серверу по порту 587 с использованием openssl s\_client -starttls smtp -crlf -connect server.alkamal.net:587. В процессе установлено TLS-соединение, отображена информация о самоподписанном сертификате, после чего сервер успешно принял команды EHLO и объявил поддержку AUTH PLAIN ([рис. 18](#fig-20)).

|  |
| --- |
| Рисунок 18: Установление SMTP over TLS соединения через openssl |

Проверка аутентификации выполнена командой AUTH PLAIN <base64>, сервер вернул ответ 235 2.7.0 Authentication successful, что подтверждает корректную работу SMTP over TLS с SASL-аутентификацией ([рис. 19](#fig-21)).

|  |
| --- |
| Рисунок 19: Успешная SMTP-аутентификация через порт 587 |

В почтовом клиенте Evolution настроен SMTP-сервер с использованием порта 587, режима STARTTLS и обычного пароля, после чего отправлено тестовое сообщение с темой «test 5» ([рис. 20](#fig-22)).

|  |
| --- |
| Рисунок 20: Отправка письма через Evolution по SMTP over TLS |

На сервере выполнена проверка почтового ящика командой MAIL=~/Maildir/ mail, где отображается сообщение с темой «test 5», что подтверждает корректную доставку письма через защищённое соединение SMTP over TLS ([рис. 21](#fig-23)).

|  |
| --- |
| Рисунок 21: Подтверждение доставки письма в Maildir |

## 2.4 Внесение изменений в настройки внутреннего

На виртуальной машине **server** выполнен переход в каталог /vagrant/provision/server, после чего конфигурационные файлы dovecot.conf, 10-master.conf, 10-auth.conf, а также master.cf Postfix скопированы в соответствующие подкаталоги mail/etc/dovecot/ и mail/etc/postfix/. Это обеспечивает сохранение рабочей конфигурации служб для последующего автоматического развёртывания через provisioning ([рис. 22](#fig-24)).

|  |
| --- |
| Рисунок 22: Копирование конфигурационных файлов Dovecot и Postfix в каталог provision |

В файл /vagrant/provision/server/mail.sh внесены изменения расширенной конфигурации SMTP-сервера: добавлена установка пакетов postfix, dovecot, telnet; копирование конфигурации в /etc; настройка firewall для служб smtp, pop3, pop3s, imap, imaps, smtp-submission; параметры Postfix (mydomain, myorigin, inet\_protocols, inet\_interfaces, mydestination); поддержка Maildir (home\_mailbox = Maildir/); SASL-аутентификация через Dovecot (smtpd\_sasl\_type, smtpd\_sasl\_path); ограничения smtpd\_recipient\_restrictions; параметр mynetworks; а также конфигурация SMTP over TLS с указанием сертификата, ключа и уровня безопасности. В конце скрипта выполняются postfix set-permissions, restorecon, перезапуск служб Postfix и Dovecot ([рис. 23](#fig-25)).

|  |
| --- |
| Рисунок 23: Расширенная конфигурация SMTP-сервера в mail.sh (server) |

В файл /vagrant/provision/client/mail.sh добавлена установка пакета telnet командой dnf -y install telnet, что обеспечивает возможность тестирования SMTP-соединения с клиента в процессе автоматической настройки виртуальной машины ([рис. 24](#fig-26)).

|  |
| --- |
| Рисунок 24: Добавление установки telnet в mail.sh (client) |

# 3. Выводы

В ходе работы выполнена комплексная настройка почтового сервера на базе Postfix и Dovecot с поддержкой LMTP, SASL-аутентификации и SMTP over TLS.

Реализована доставка почты через LMTP-сокет Dovecot, что обеспечило корректную интеграцию MTA и MDA. Настроена SASL-аутентификация через Dovecot, исключающая несанкционированное использование сервера в качестве SMTP-relay. Ограничения smtpd\_recipient\_restrictions и параметр mynetworks обеспечили контроль приёма сообщений.

Настроена поддержка TLS с использованием сертификата Dovecot и реализован сервис submission (порт 587) с обязательным шифрованием и аутентификацией. Проверка через openssl и AUTH PLAIN подтвердила успешное установление защищённого соединения.

Отправка сообщений через telnet и почтовый клиент Evolution показала корректную работу SMTP over TLS и доставку писем в Maildir пользователя.

Конфигурация интегрирована в механизм provisioning виртуальной машины, что обеспечивает воспроизводимость настройки внутреннего окружения.

# 4. 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?

* Почтовый Relay-сервер выполняет функции пересылки почты от одного почтового сервера к другому, облегчая маршрутизацию электронных сообщений между различными почтовыми системами.

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

Угрозы безопасности, связанные с настройкой почтового сервера как Relay-сервера, могут включать рассылку нежелательной почты (спам), перехват и изменение электронных сообщений, а также использование сервера для ретрансляции вредоносных сообщений.