**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЁТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №10**

*дисциплина: Администрирование сетевых подсистем*

Студент: Бансимба Клодели Дьегра

Студ. билет № 1032215651

Группа: НПИбд-02-22

**МОСКВА**

2024 г.

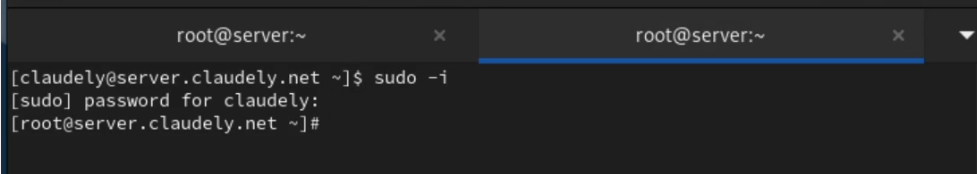
# Цель работы:

# Целью данной работы является приобретение практических навыков по конфигурированию SMTP-сервера в части настройки аутентификации.

**Выполнение работы:**

На виртуальной машине server войдём под нашим пользователем и откроем терминал. Перейдём в режим суперпользователя (Рис. 1.1):

sudo -i

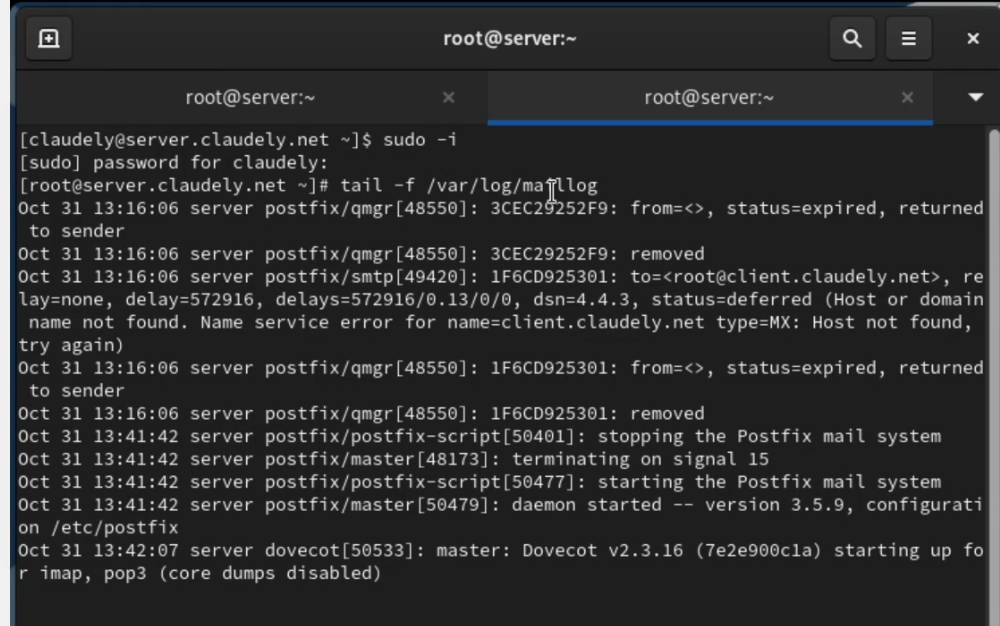
****

**Рис. 1.1.** Открытие режима суперпользователя на виртуальной машине server.

В дополнительном терминале запустим мониторинг работы почтовой службы (Рис. 1.2):

sudo -i

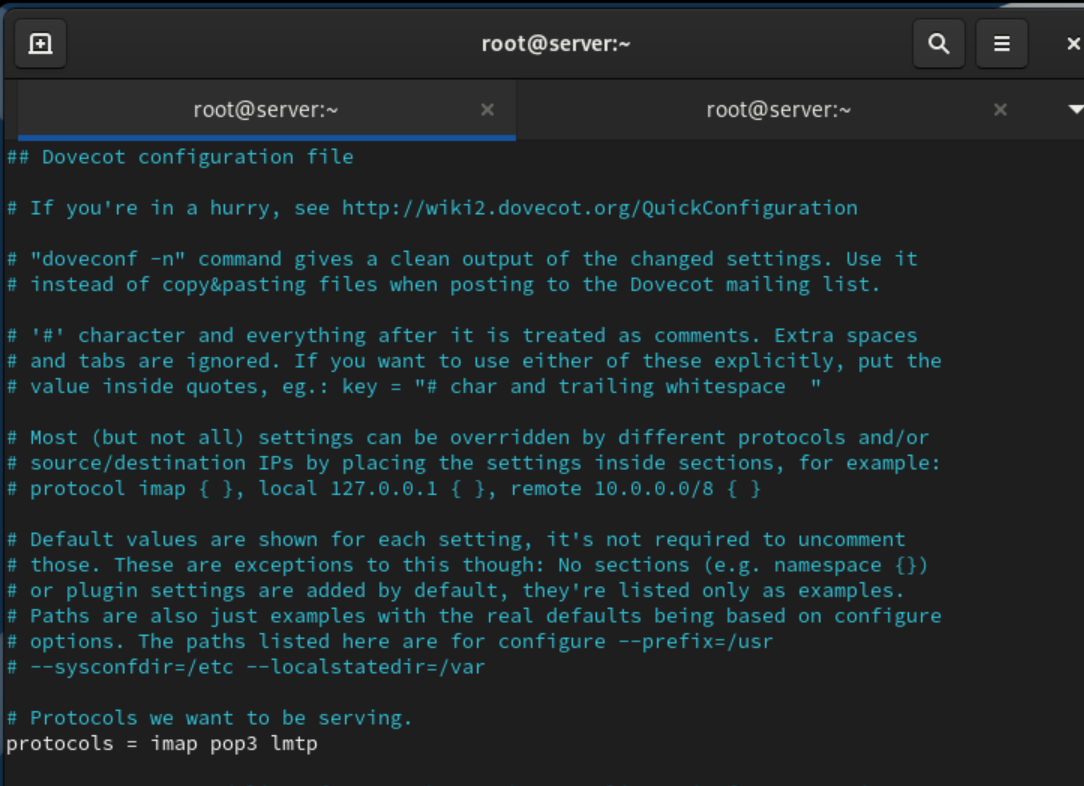
tail -f /var/log/maillog

****

**Рис. 1.2.** Запуск в дополнительном терминале мониторинга работы почтовой службы.

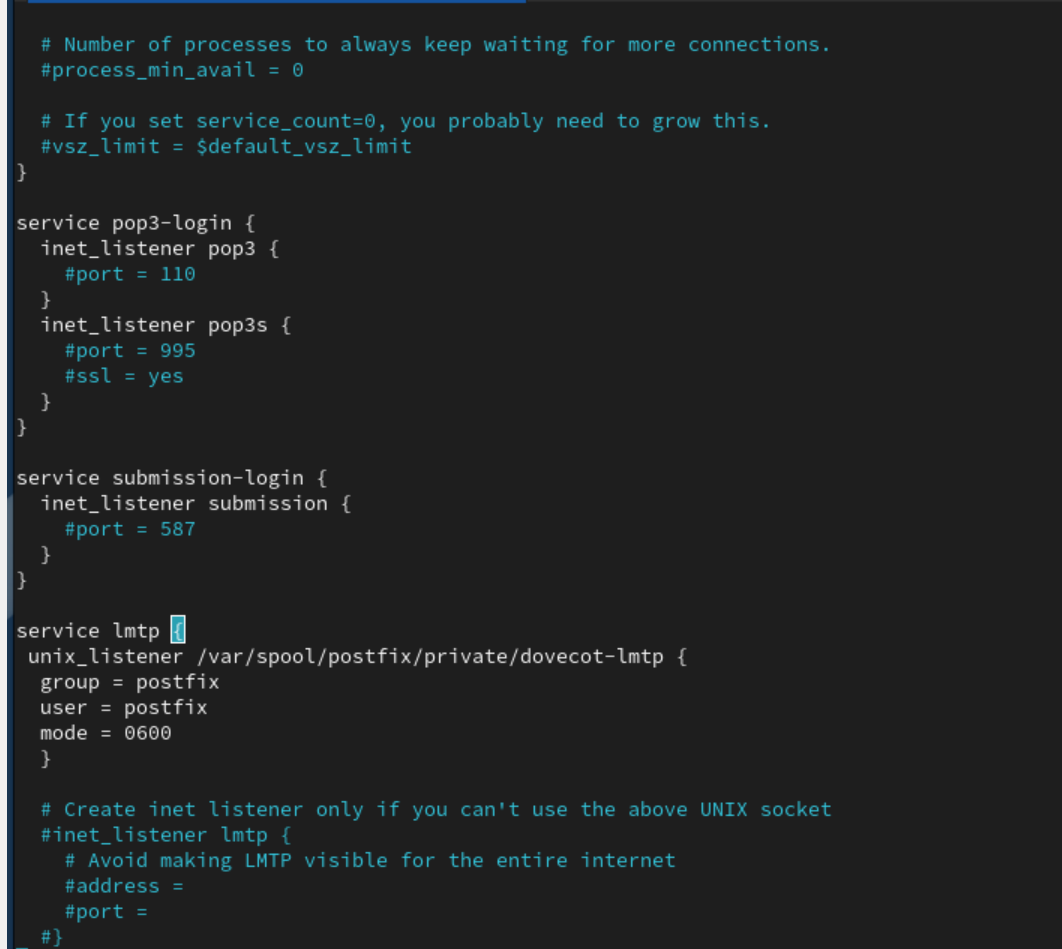
Добавим в список протоколов, с которыми может работать Dovecot, протокол LMTP. Для этого в файле /etc/dovecot/dovecot.conf укажем (Рис. 1.3):

protocols = imap pop3 lmtp

****

**Рис. 1.3.** Добавление в список протоколов, с которыми может работать Dovecot, протокола LMTP.

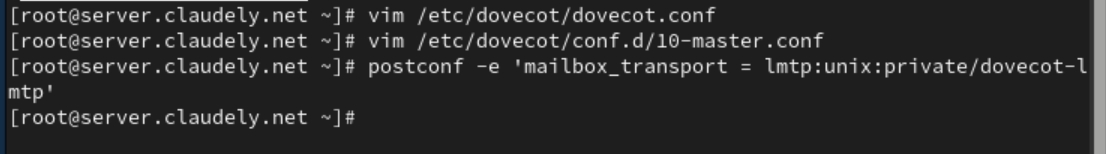
Настроим в Dovecot сервис lmtp для связи с Postfix. Для этого в файле /etc/dovecot/conf.d/10-master.conf замените определение сервиса lmtp на следующую запись из лабораторной работы (Рис. 1.4). Эта запись определяет расположение файла с описанием прослушиваемого unix-сокета, а также задаёт права доступа к нему и определяет принадлежность к группе и пользователю postfix.



**Рис. 1.4.** Настройка в Dovecot сервиса lmtp для связи с Postfix.

Переопределим в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокет (Рис. 1.5):

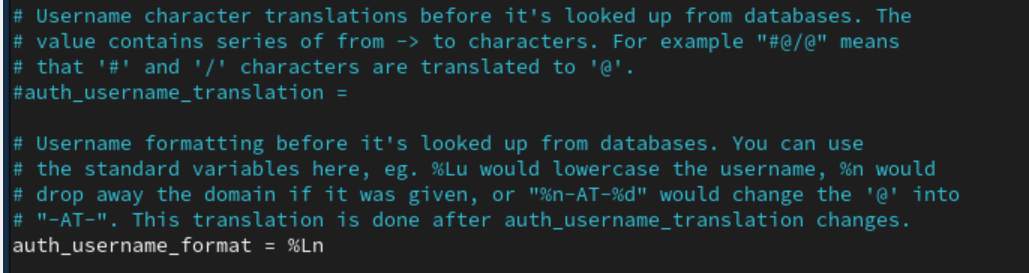
postconf -e 'mailbox\_transport = lmtp:unix:private/dovecot-lmtp'

****

**Рис. 1.5.** Переопределение в Postfix с помощью postconf передачи сообщений не на прямую, а через заданный unix-сокет.

В файле /etc/dovecot/conf.d/10-auth.conf зададим формат имени пользователя для аутентификации в форме логина пользователя без указания домена (Рис. 1.6):

auth\_username\_format = %Ln

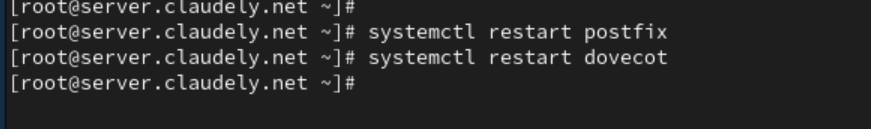


**Рис. 1.6.** Настройка в файле /etc/dovecot/conf.d/10-auth.conf формата имени пользователя для аутентификации в форме логина пользователя без указания домена.

Перезапустим Postfix и Dovecot (Рис. 1.7):

systemctl restart postfix

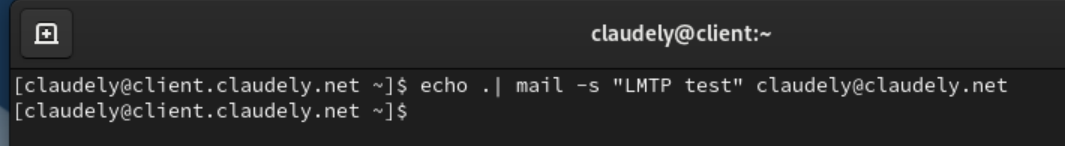
systemctl restart dovecot



**Рис. 1.7.** Перезапуск Postfix и Dovecot.

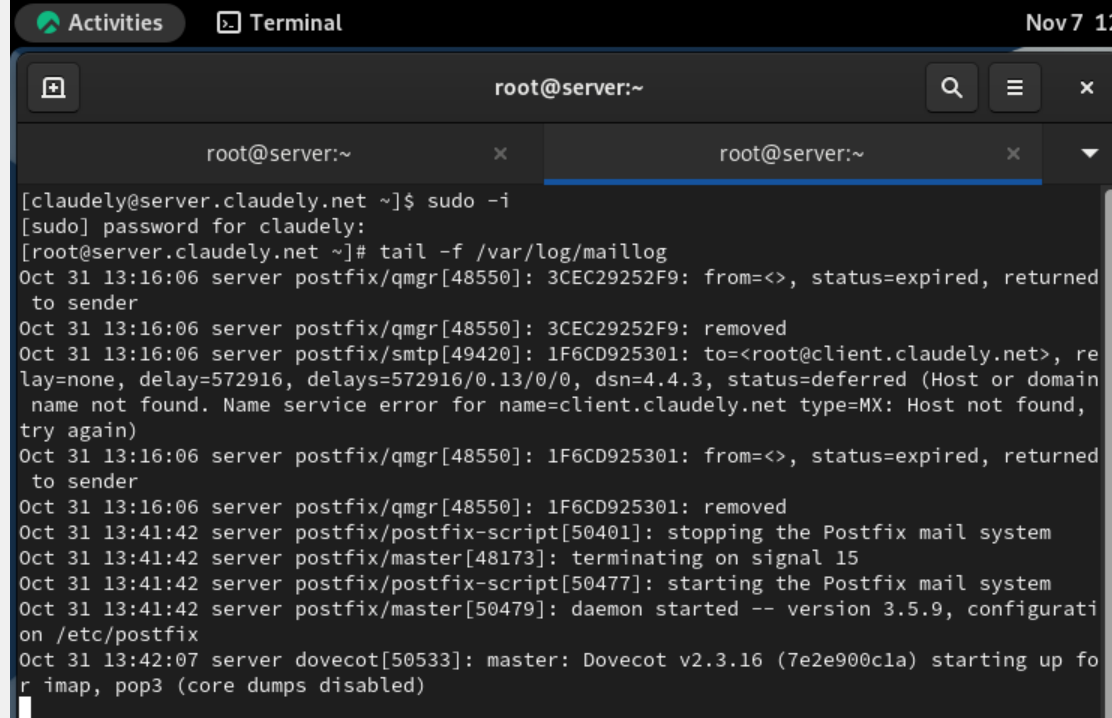
Из-под учётной записи своего пользователя отправим письмо с клиента (Рис. 1.8):

echo .| mail -s "LMTP test" claudely@claudely.net



**Рис. 1.8.** Отправка из-под учётной записи своего пользователя письма с клиента.

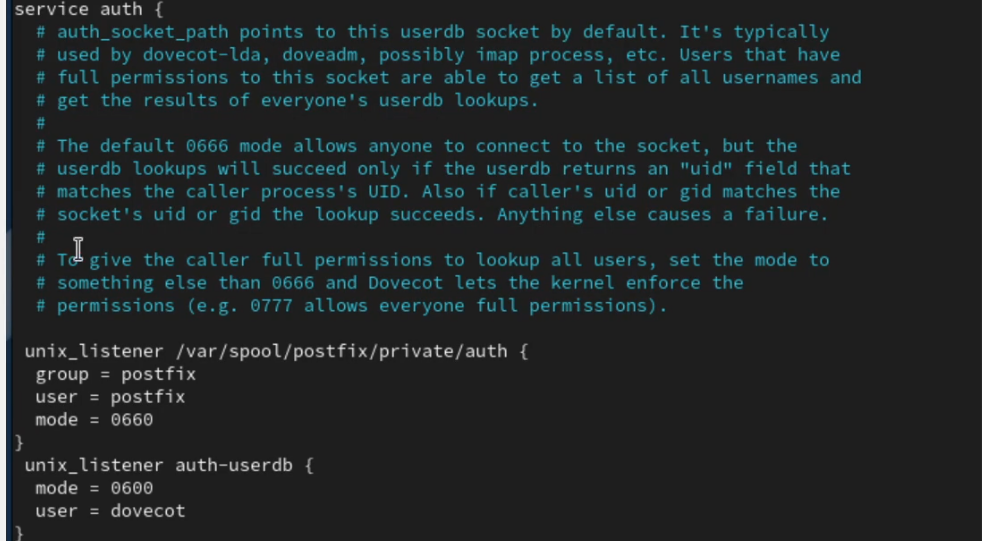
После чего посмотрим содержание логов при мониторинге почтовой службы (Рис. 1.9):



**Рис. 1.9.**  Просмотр содержания логов при мониторинге почтовой службы.

**Рис. 1.10.** Просмотр на сервере почтового ящика пользователя.

В файле /etc/dovecot/conf.d/10-master.conf определим службу аутентификации пользователей (Рис. 2.1):



**Рис. 2.1.** Определение в файле /etc/dovecot/conf.d/10-master.conf службы аутентификации пользователей.

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

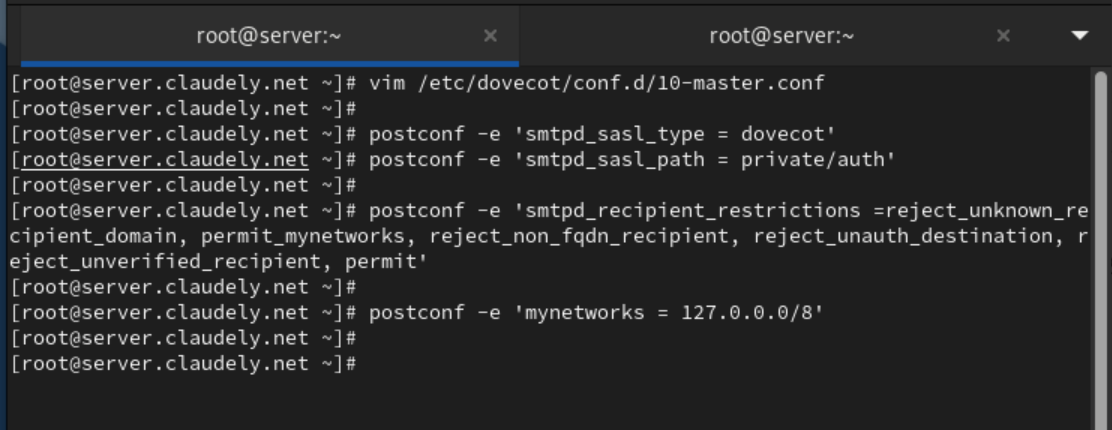
postconf -e 'smtpd\_sasl\_type = dovecot' postconf -e 'smtpd\_sasl\_path = private/auth'

Далее 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'

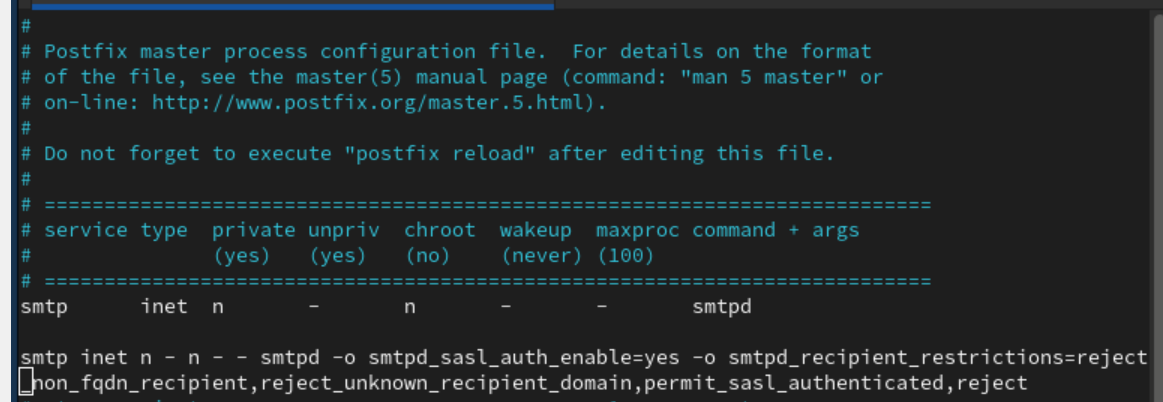
В настройках Postfix ограничим приём почты только локальным адресом SMTP-сервера сети (Рис. 2.2):

postconf -e 'mynetworks = 127.0.0.0/8'



**Рис. 2.2.** Настройка для Postfix типа аутентификации SASL для smtpd и пути к соответствующему unix-сокету, настройка Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины, ограничение в настройках Postfix приёма почты только локальным адресом SMTP-сервера сети.

Для проверки работы аутентификации временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Для этого в файле /etc/postfix/master.cf заменим строку (Рис. 2.3):

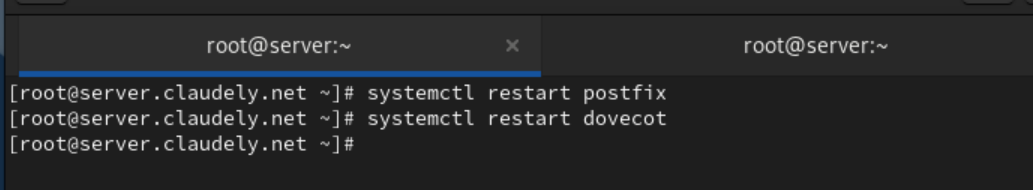


**Рис. 2.3.** Временный запуск для проверки работы аутентификации SMTP-сервера (порт 25) с возможностью аутентификации.

Затем перезапустим Postfix и Dovecot (Рис. 2.4):

systemctl restart postfix

systemctl restart dovecot

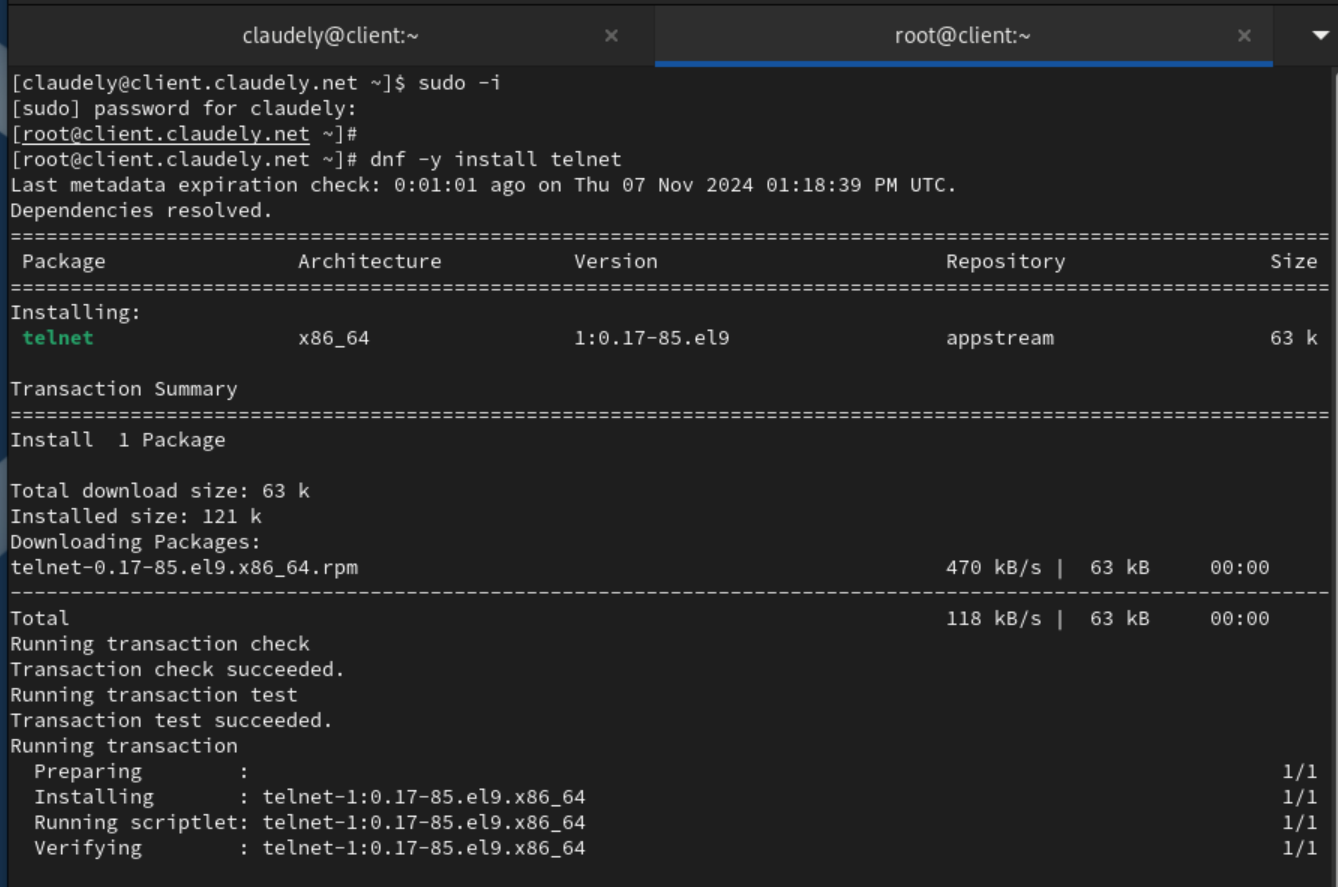


**Рис. 2.4.** Перезапуск Postfix и Dovecot.

На клиенте установим telnet (Рис. 2.5):

sudo -i

dnf -y install telnet



**Рис. 2.5.** Установка на клиенте telnet.

На клиенте получим строку для аутентификации:

printf 'claudely\x00username\x00123456' | base64

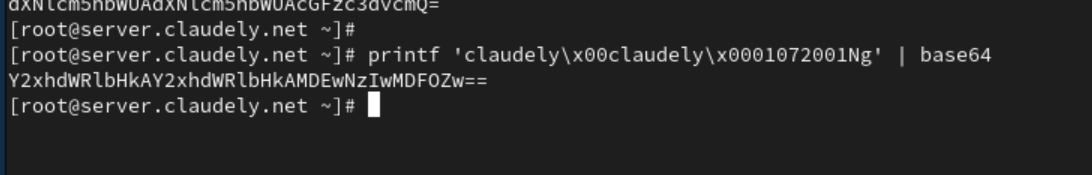
В качестве результата получим строку для аутентификации в формате base64. После чего подключимся на клиенте к SMTP-серверу посредством telnet:

telnet server.claudely.net 25

Теперь протестируем соединение, введя EHLO test и проверим авторизацию, задав:

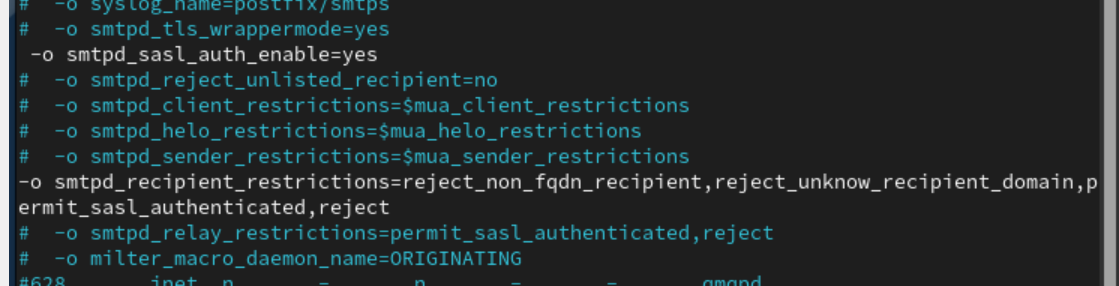
AUTH PLAIN <СДА>

Завершим сессию telnet на клиенте (Рис. 2.6):



**Рис. 2.6.** Получение на клиенте строки для аутентификации, подключение на клиенте к SMTP-серверу посредством telnet, тестирование соединения, проверка авторизации и завершение сессии telnet на клиенте.

Для того чтобы запустить SMTP-сервер на 587-м порту, в файле /etc/postfix/master.cf заменим строки (рис. 3.2):



**Рис. 3.2.** Замена строк в файле /etc/postfix/master.cf для того чтобы запустить SMTP-сервер на 587-м порту.

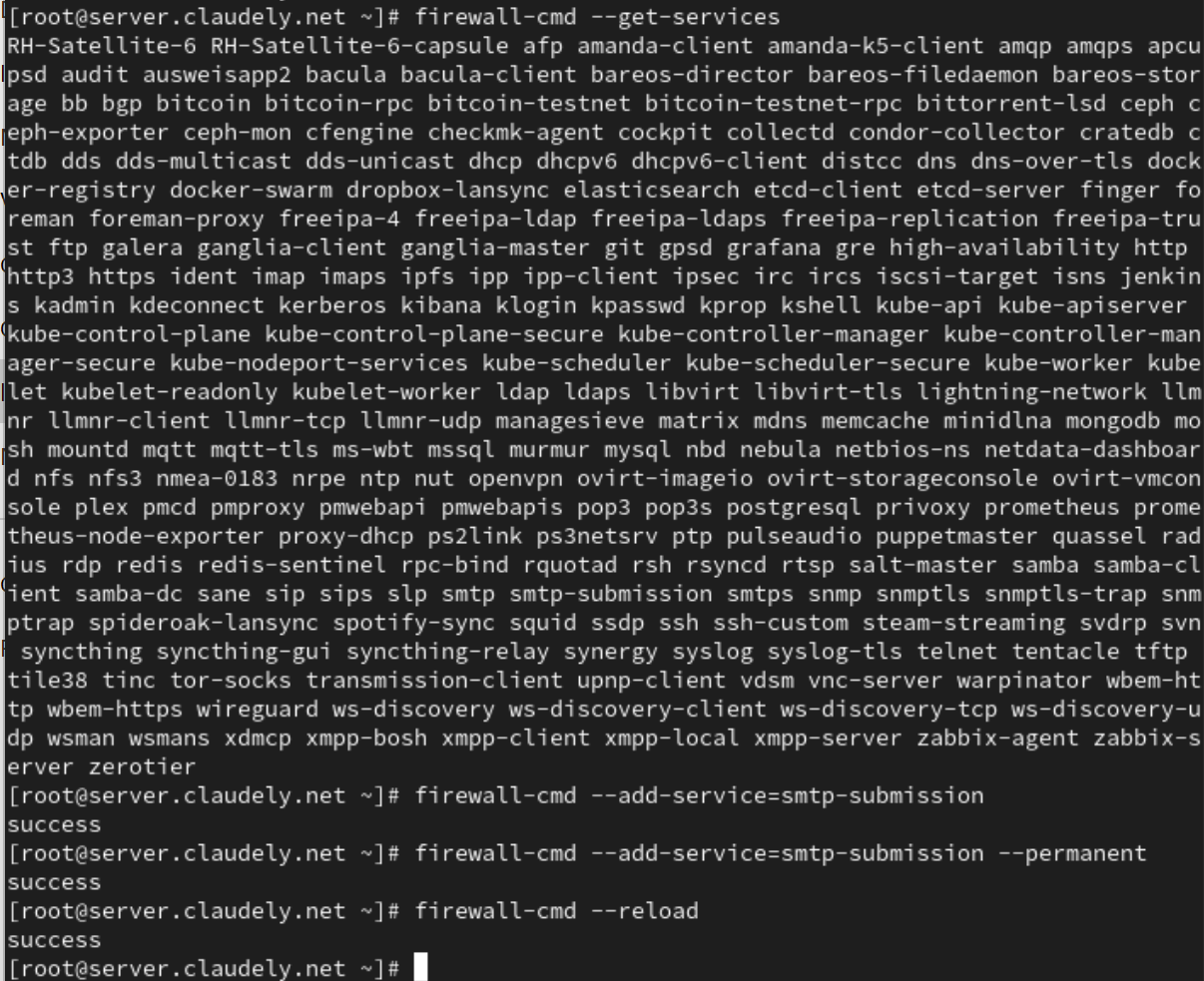
Настроим межсетевой экран, разрешив работать службе smtp-submission (рис. 3.3):

firewall-cmd --get-services

firewall-cmd --add-service=smtp-submission

firewall-cmd --add-service=smtp-submission --permanent

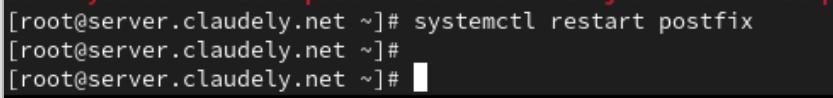
firewall-cmd --reload



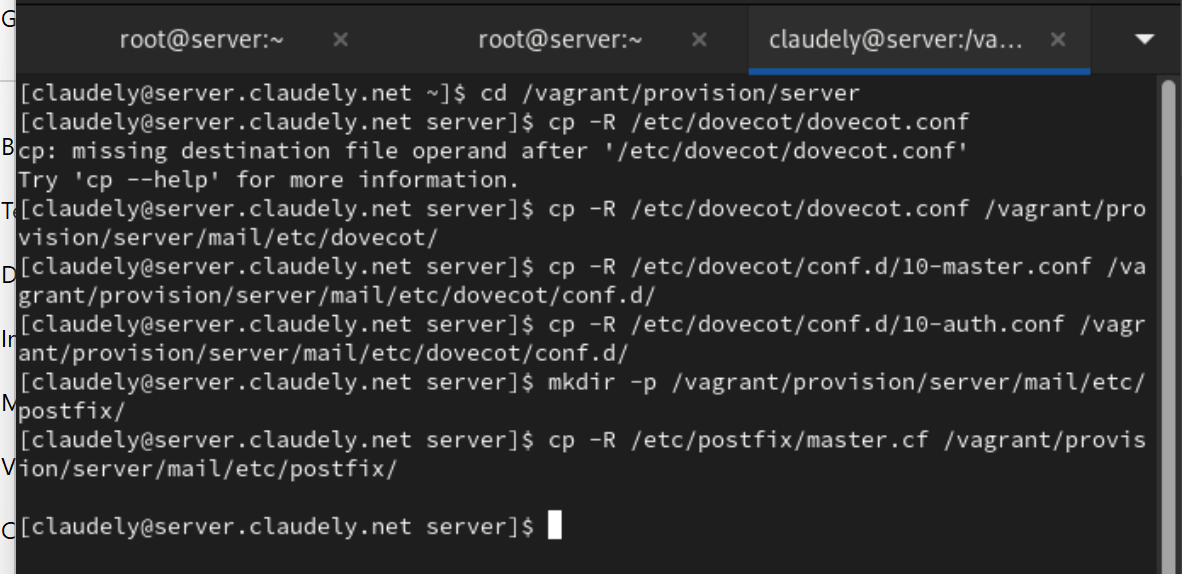
**Рис. 3.3.** Настройка межсетевого экрана, разрешив работать службе smtp-submission.

Перезапустим Postfix (рис. 3.4):

systemctl restart postfix

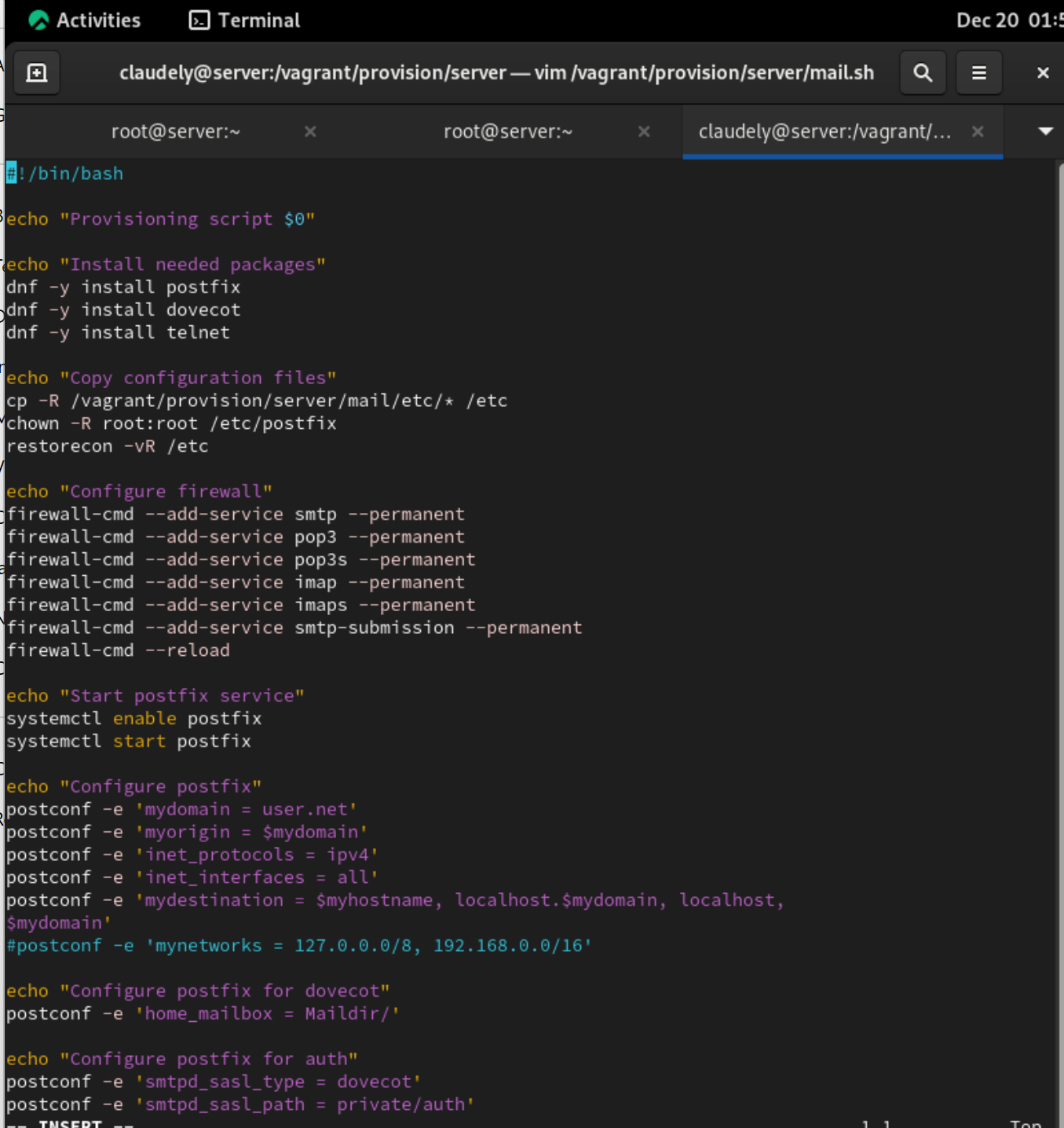


**Рис. 3.4.** Перезапуск Postfix.



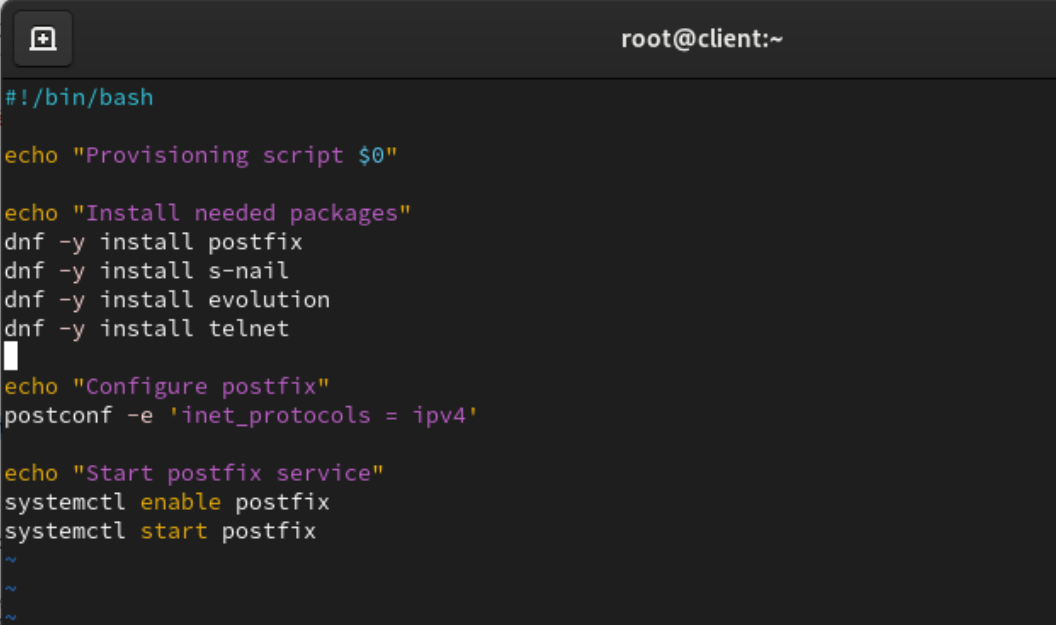
**Рис. 4.1.** Переход в каталог на виртуальной машине server для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и помещение в соответствующие подкаталоги конфигурационных файлов Dovecot и Postfix.

Внесём соответствующие изменения по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh (рис. 4.2):



**Рис. 4.2.** Внесение соответствующих изменений по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh.

Внесём изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet (Рис. 4.3):



**Рис. 4.3.** Внесение изменения в файл /vagrant/provision/client/mail.sh.

**Вывод:**

# В ходе выполнения лабораторной работы были приобретены практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

**Ответы на контрольные вопросы:**

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

**Допустим, у нас есть почтовый ящик с адресом user@example.com. В конфигурационном файле Dovecot (/etc/dovecot/conf.d/10-auth.conf), мы можем указать формат аутентификации следующим образом:**

**auth\_username\_format = %Lu**

**В этом примере %Lu означает, что аутентификация будет проходить в формате "user" без учета регистра букв. Если вам нужно учитывать домен, вы можете использовать %n:**

**auth\_username\_format = %Ln**

**Таким образом, при вводе логина "user@example.com" пользователь будет аутентифицироваться с именем пользователя "user" и доменом "example.com".**

1. Какие функции выполняет почтовый Relay-сервер? **–**

**Пересылка почты: Relay-сервер принимает почтовые сообщения от клиентов и пересылает их к адресатам. Это особенно полезно, если у вас нет прямого доступа к серверу назначения или если вы хотите централизованно управлять отправкой почты.**

**Маршрутизация почты: Relay-сервер может определять наилучший маршрут для доставки почты на основе определенных правил и политик.**

**Блокировка спама: Некоторые Relay-серверы выполняют функции фильтрации спама, блокируя нежелательные сообщения до их отправки на сервер назначения.**

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

**Открытый Relay: Если сервер настроен как открытый Relay, это может привести к злоупотреблению. Злоумышленники могут использовать сервер для отправки спама, что может повлечь за собой блокировку IP-адреса сервера или другие санкции.**

**Спуфинг: Атаки, связанные с подделкой отправителя (спуфинг), могут быть использованы для маскировки настоящего источника почты. Это может быть проблемой, если сервер Relay доверяет внешним источникам без должной аутентификации.**

**Отказ в обслуживании (DoS): Атаки типа DoS могут быть направлены на Relay-сервер, перегружая его запросами на пересылку почты и создавая неприемлемую загрузку.**