Лабораторная работа №10

Расширенные настройки SMTP-сервера

Студент: Пакавира Арсениу Висенте Луиш

Группа: НФИбд 02–23

дисциплина: **Администрирование сетевых подсистем (Lab 10)**

Цель работы

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

Настройка LMTP в Dovecote

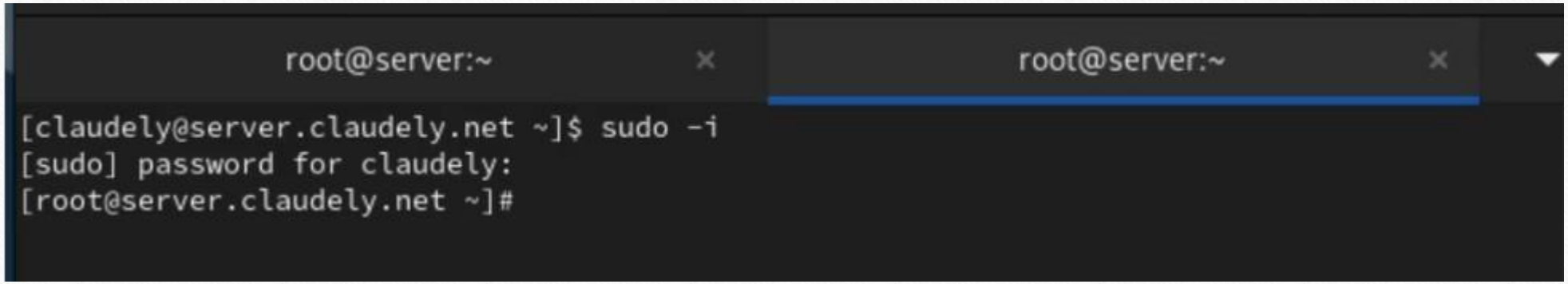

Рис. 1.1. Открытие режима суперпользователя на виртуальной машине server.

Настройка LMTP в Dovecote

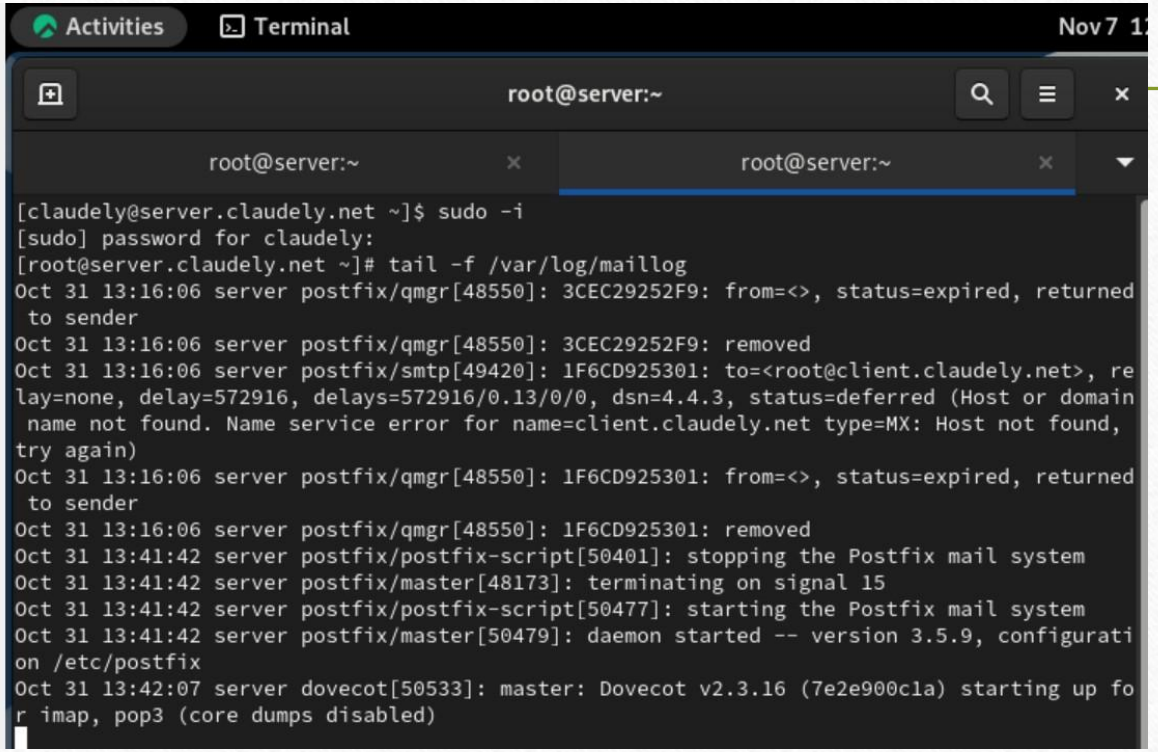

Рис. 1.2. Запуск в дополнительном терминале мониторинга работы почтовой службы.

Настройка LMTP в Dovecote

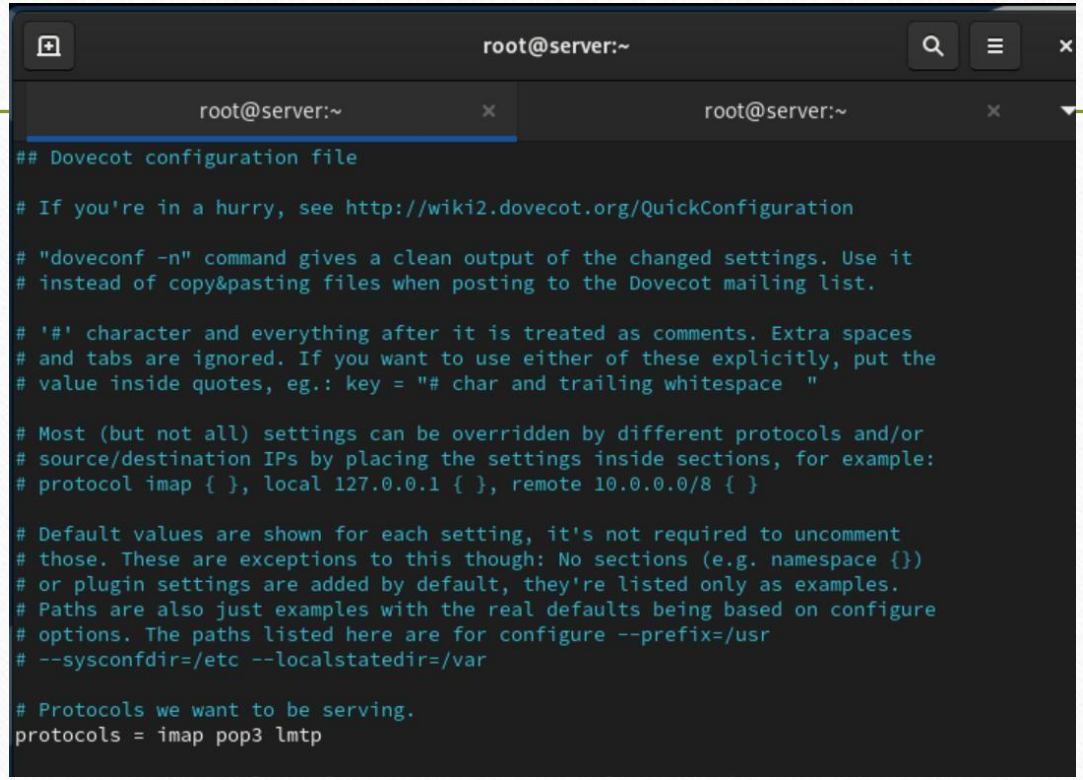

Рис. 1.3. Добавление в список протоколов, с которыми может работать Dovecot, протокола LMTP.

Настройка LMTP в Dovecote

```
  # Number of processes to always keep waiting for more connections.
  #process_min_avail = 0

  # If you set service_count=0, you probably need to grow this.
  #vsz_limit = $default_vsz_limit
}

service pop3-login {
  inet_listener pop3 {
    #port = 110
  }
  inet_listener pop3s {
    #port = 995
    #ssl = yes
  }
}

service submission-login {
  inet_listener submission {
    #port = 587
  }
}

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

  # Create inet listener only if you can't use the above UNIX socket
  #inet_listener lmtp {
    # Avoid making LMTP visible for the entire internet
    #address =
    #port =
  #}
```

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

Настройка LMTP в Dovecote

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

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

Настройка LMTP в Dovecote

```
# Username character translations before it's looked up from databases. The
# value contains series of from -> to characters. For example "#@/@" means
# that '#' and '/' characters are translated to '@'.
#auth_username_translation =

# Username formatting before it's looked up from databases. You can use
# the standard variables here, eg. %Lu would lowercase the username, %n would
# drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
# "-AT-". This translation is done after auth_username_translation changes.
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.

Настройка LMTP в Dovecote

```
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# systemctl restart postfix
[root@server.claudely.net ~]# systemctl restart dovecot
[root@server.claudely.net ~]#
```

Рис. 1.7. Перезапуск Postfix и Dovecot.

Настройка LMTP в Dovecote

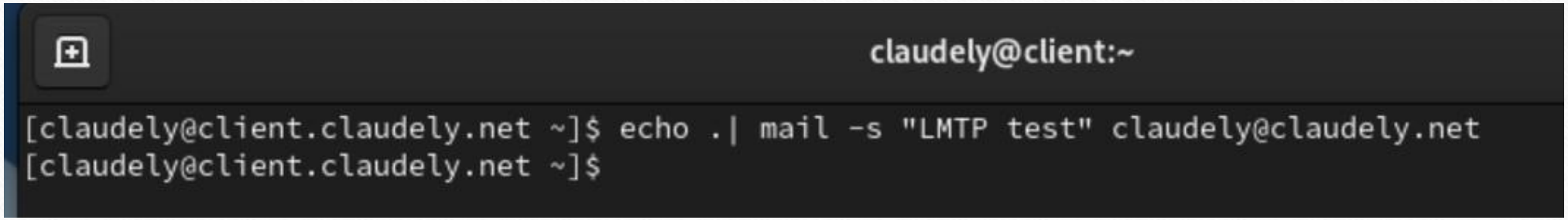

Рис. 1.8. Отправка из-под учётной записи своего пользователя письма с клиента.

Настройка SMTP-аутентификации

```
  # something else than 0666 and Dovecot lets the kernel enforce the
  # permissions (e.g. 0777 allows everyone full permissions).

 unix_listener /var/spool/postfix/private/auth {
  group = postfix
  user = postfix
  mode = 0660
}
 unix_listener auth-userdb {
  mode = 0600
  user = dovecot
}
}
  # Postfix smtp-auth
  #unix_listener /var/spool/postfix/private/auth {
  #  mode = 0666
  #}
```

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

Настройка SMTP-аутентификации

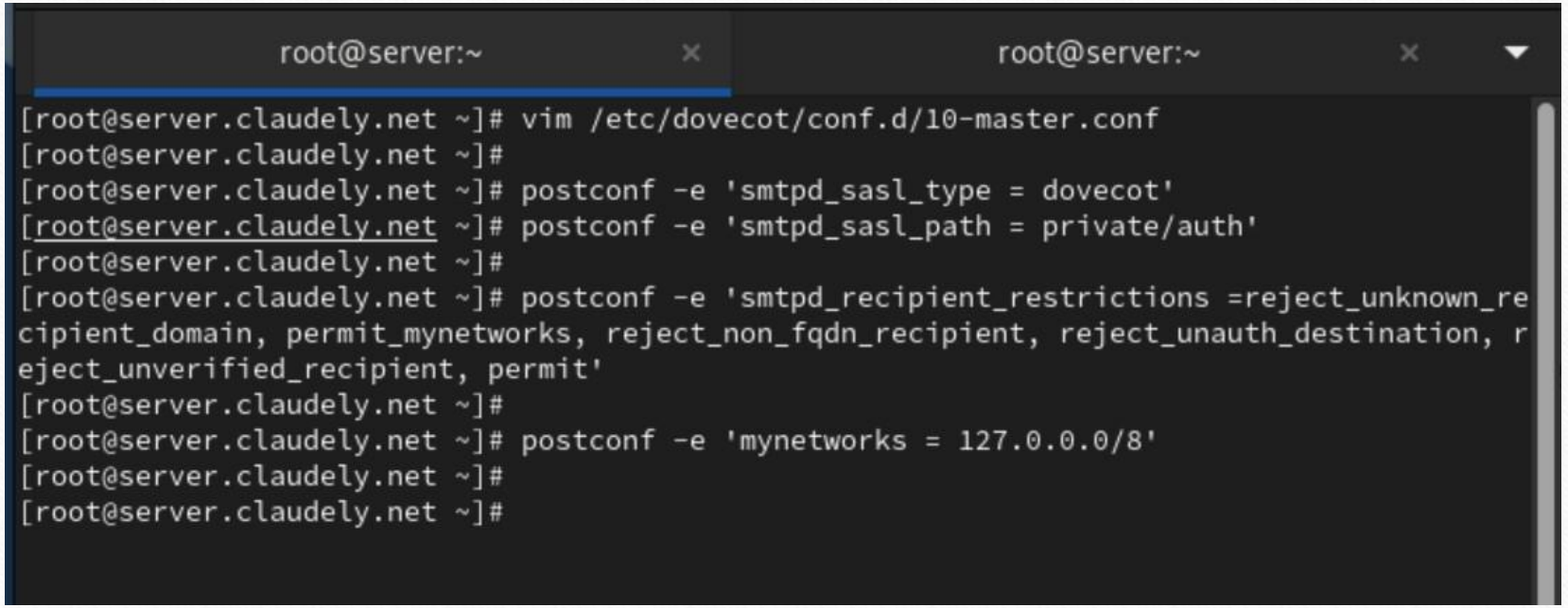

Рис. 2.2. Настройка для Postfix типа аутентификации SASL для smtpd и пути к соответствующему unix-сокету, настройка Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины, ограничение в настройках Postfix приёма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

Настройка SMTP-аутентификации

```
#
# 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

smtp inet n - n - - smtpd -o smtpd_sasl_auth_enable=yes -o smtpd_recipient_restrictions=reject
non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
```

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

Настройка SMTP-аутентификации

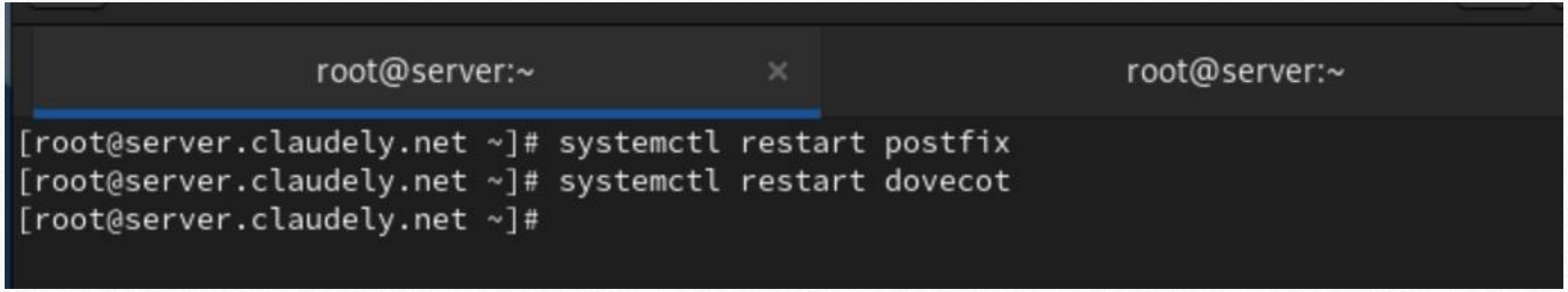

Рис. 2.4. Перезапуск Postfix и Dovecot.

Настройка SMTP-аутентификации

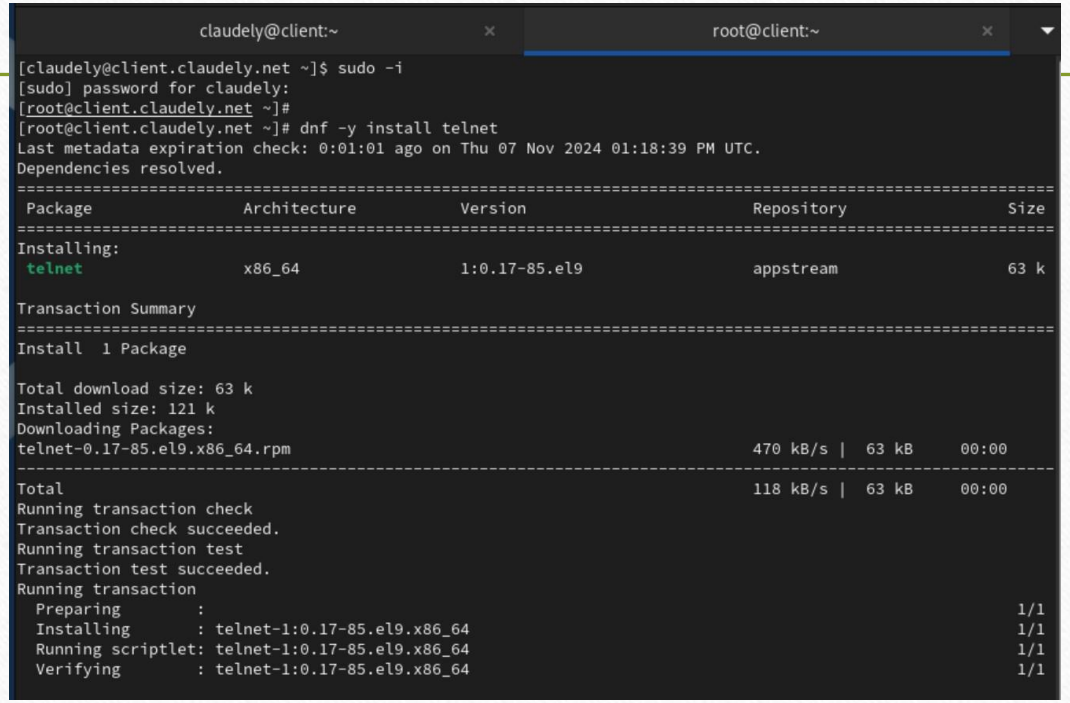

Рис. 2.5. Установка на клиенте telnet.

Настройка SMTP-аутентификации

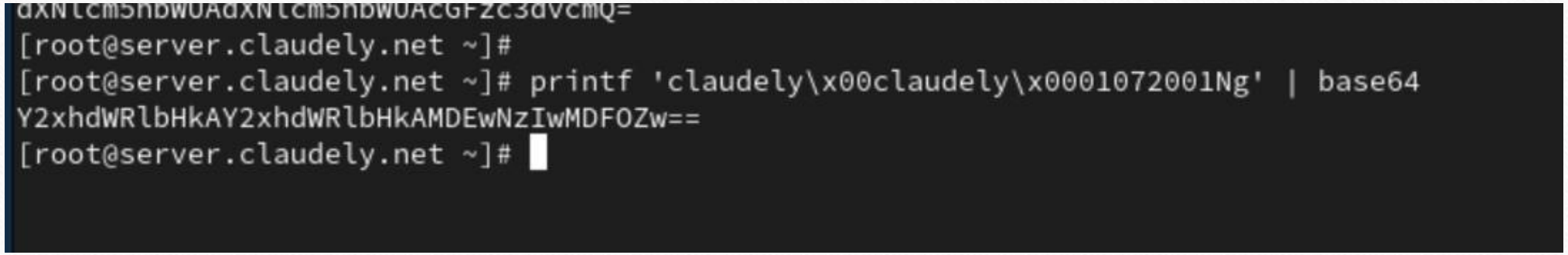

Рис. 2.6. Получение на клиенте строки для аутентификации, подключение на клиенте к SMTP-серверу посредством telnet, тестирование соединения, проверка авторизации и завершение сессии telnet на клиенте.

Настройка SMTP over TLS

```
#  -o syslog_name=postfix/smtps
#  -o smtpd_tls_wrappermode=yes
 -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknow_recipient_domain,p
ermit_sasl_authenticated,reject
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
```

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

Настройка SMTP over TLS

```
[root@server.claudely.net ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcu
psd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-stor
age bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph c
eph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb c
tdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls dock
er-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger fo
reman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-tru
st ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http
http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkin
s kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver
kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-man
ager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kube
let kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llm
nr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mo
sh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboar
d nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmcon
sole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prome
theus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel rad
ius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-cl
ient samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn
 syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp
tile38 tinc tor-socks transmission-client upnp-client vdsm vnc-server warpinator wbem-ht
tp wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-u
dp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-s
erver zerotier
[root@server.claudely.net ~]# firewall-cmd --add-service=smtp-submission
success
[root@server.claudely.net ~]# firewall-cmd --add-service=smtp-submission --permanent
success
[root@server.claudely.net ~]# firewall-cmd --reload
success
[root@server.claudely.net ~]#
```

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

Настройка SMTP over TLS

```
[root@server.claudely.net ~]# systemctl restart postfix
[root@server.claudely.net ~]#
[root@server.claudely.net ~]#
```

Рис. 3.4. Перезапуск Postfix.

Внесение изменений в настройки внутреннего окружения виртуальной машины

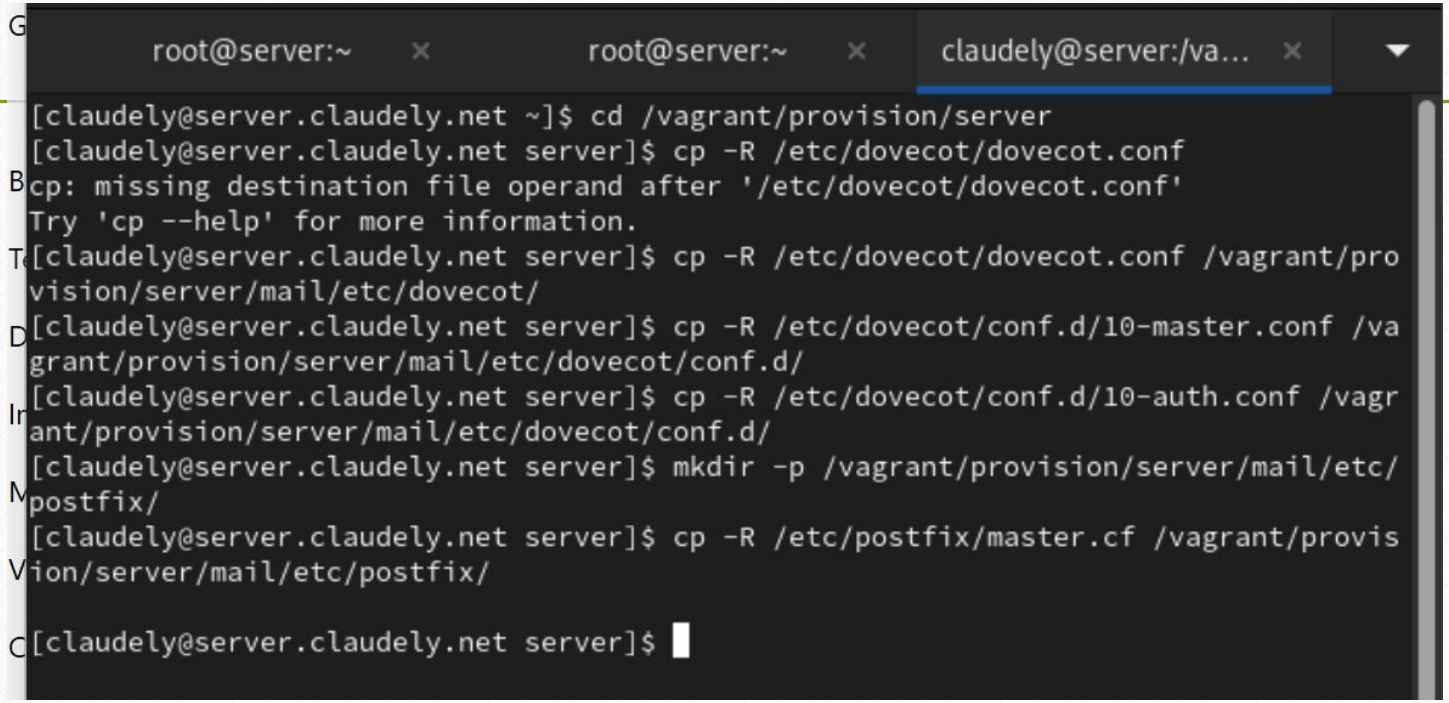

Рис. 4.1. Переход в каталог на виртуальной машине server для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и помещение в соответствующие подкаталоги конфигурационных файлов Dovecot и Postfix.

Внесение изменений в настройки внутреннего окружения виртуальной машины

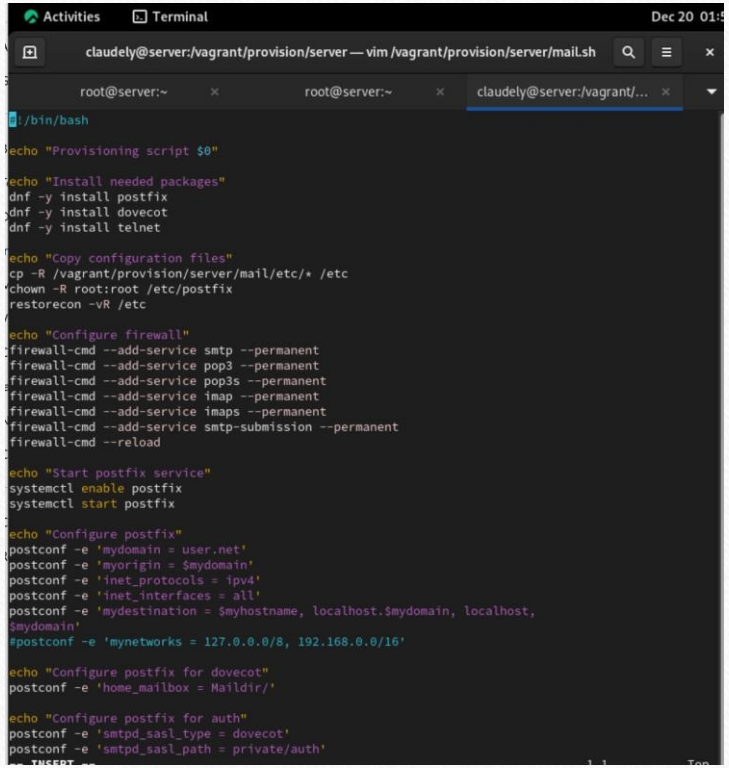

Рис. 4.2. Внесение соответствующих изменений по расширенной конфигурации SMTP-сервера в файл /vagrant/provision/server/mail.sh.

Внесение изменений в настройки внутреннего окружения виртуальной машины

root@client:~

```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install postfix
dnf -y install s-nail
dnf -y install evolution
dnf -y install telnet

echo "Configure postfix"
postconf -e 'inet_protocols = ipv4'

echo "Start postfix service"
systemctl enable postfix
systemctl start postfix
```

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.

Спасибо за внимание!