

Лабораторная работа

№10

Расширенные настройки SMTP-сервера

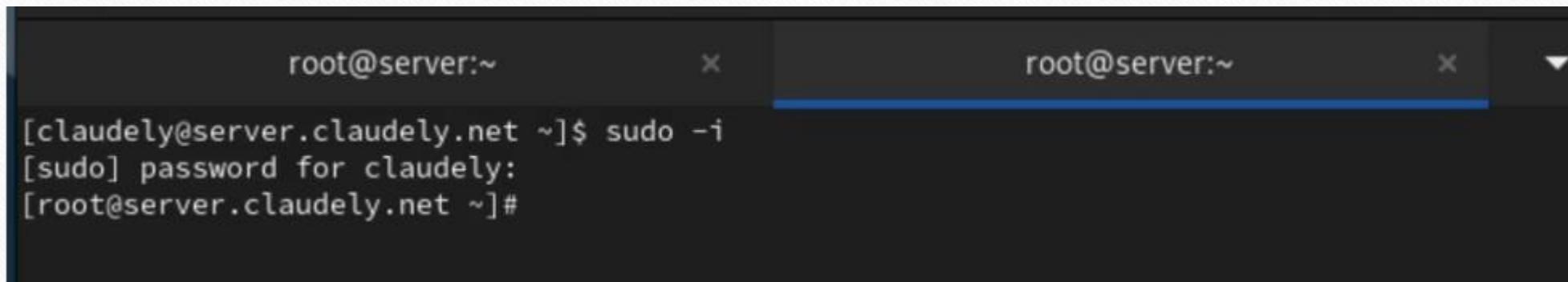
Студент: Пакавира Арсениу Висенте Луиш
Группа: НФИбд 02–23

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

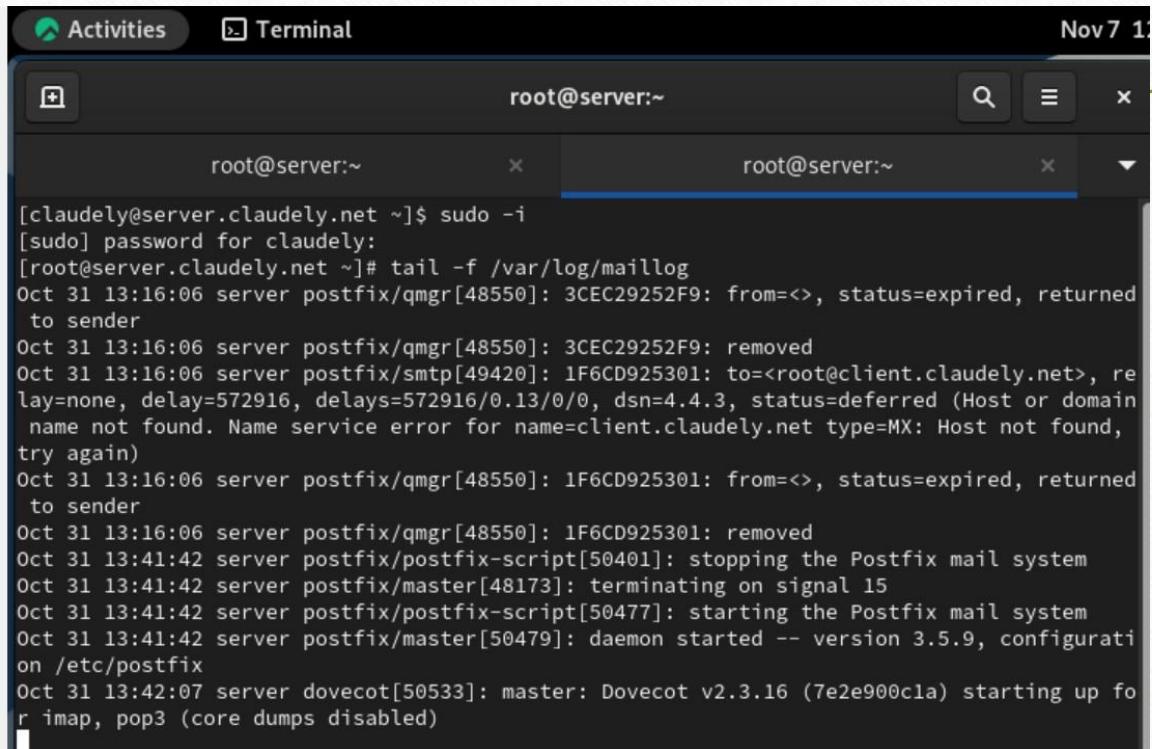


The screenshot shows two terminal windows side-by-side. Both windows have a dark background and white text. The left window shows the command `sudo -i` being entered, followed by a password prompt for the user `claudely`. The right window shows the command `sudo -i` completed, and the user has switched to the root shell, indicated by the prompt `[root@server.cludely.net ~]#`.

```
root@server:~ [claudely@server.cludely.net ~]$ sudo -i
[sudo] password for claudely:
[root@server.cludely.net ~]#
```

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

Настройка LMTP в Dovecote

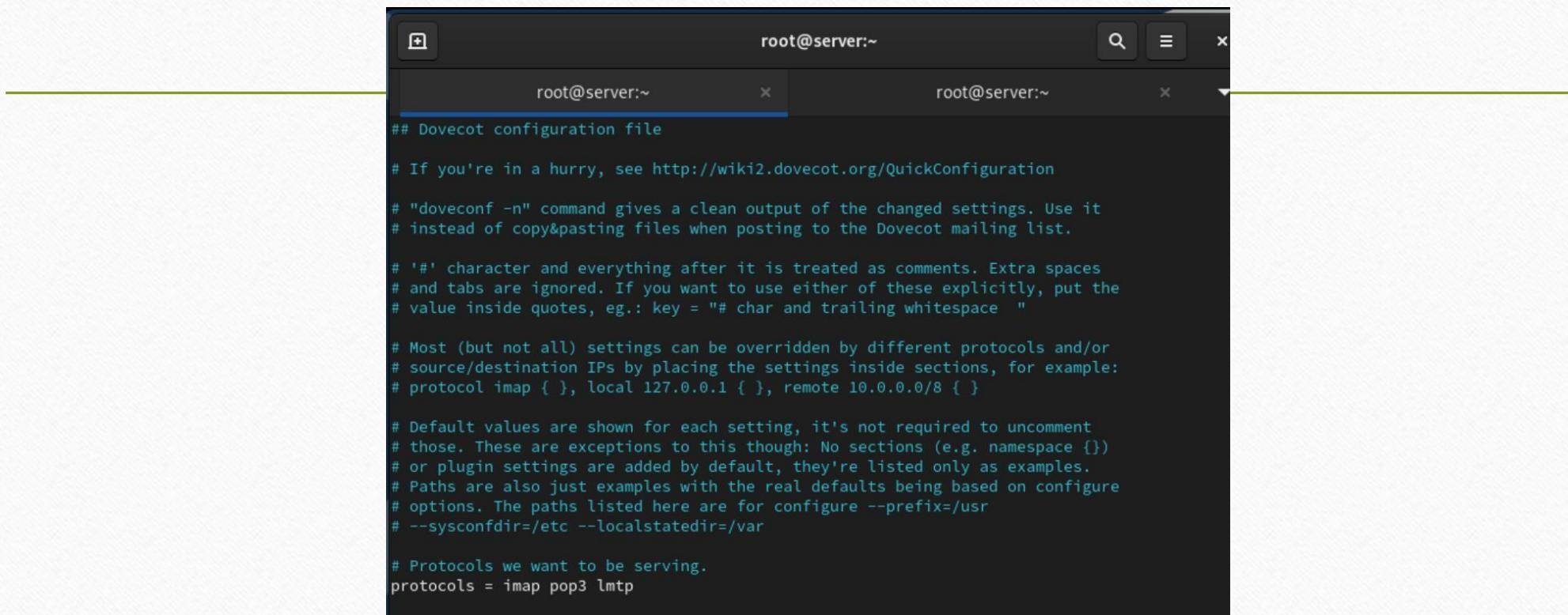


The screenshot shows a terminal window titled "Terminal" with two tabs open, both labeled "root@server:~". The window is running on a desktop environment with a dock at the bottom. The terminal displays the following command and its output:

```
[claudely@server.claudely.net ~]$ sudo -i  
[sudo] password for claudely:  
[root@server.claudely.net ~]# tail -f /var/log/maillog  
Oct 31 13:16:06 server postfix/qmgr[48550]: 3CEC29252F9: from=<>, status=expired, returned  
to sender  
Oct 31 13:16:06 server postfix/qmgr[48550]: 3CEC29252F9: removed  
Oct 31 13:16:06 server postfix/smtp[49420]: 1F6CD925301: to=<root@client.claudely.net>, re  
lay=none, delay=572916, delays=572916/0.13/0/0, dsn=4.4.3, status=deferred (Host or domain  
name not found. Name service error for name=client.claudely.net type=MX: Host not found,  
try again)  
Oct 31 13:16:06 server postfix/qmgr[48550]: 1F6CD925301: from=<>, status=expired, returned  
to sender  
Oct 31 13:16:06 server postfix/qmgr[48550]: 1F6CD925301: removed  
Oct 31 13:41:42 server postfix/postfix-script[50401]: stopping the Postfix mail system  
Oct 31 13:41:42 server postfix/master[48173]: terminating on signal 15  
Oct 31 13:41:42 server postfix/postfix-script[50477]: starting the Postfix mail system  
Oct 31 13:41:42 server postfix/master[50479]: daemon started -- version 3.5.9, configurati  
on /etc/postfix  
Oct 31 13:42:07 server dovecot[50533]: master: Dovecot v2.3.16 (7e2e900cla) starting up fo  
r imap, pop3 (core dumps disabled)
```

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

Настройка LMTP в Dovecote



The screenshot shows a terminal window with two tabs open, both titled "root@server:~". The left tab is active and displays the Dovecot configuration file. The right tab is inactive. The configuration file content is as follows:

```
## Dovecot configuration file

# If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration

# "doveconf -n" command gives a clean output of the changed settings. Use it
# instead of copy&pasting files when posting to the Dovecot mailing list.

# '#' character and everything after it is treated as comments. Extra spaces
# and tabs are ignored. If you want to use either of these explicitly, put the
# value inside quotes, eg.: key = "# char and trailing whitespace "

# Most (but not all) settings can be overridden by different protocols and/or
# source/destination IPs by placing the settings inside sections, for example:
# protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }

# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

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

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-lmtp'
[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



```
claudely@client:~  
[claudely@client.claudely.net ~]$ echo .| mail -s "LMTP test" claudely@claudely.net  
[claudely@client.claudely.net ~]$
```

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

The screenshot shows two terminal windows side-by-side, both titled "root@server:~". The left window contains the following command sequence:

```
[root@server.claudely.net ~]# vim /etc/dovecot/conf.d/10-master.conf
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server.claudely.net ~]# postconf -e 'smtpd_sasl_path = private/auth'
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# postconf -e 'smtpd_recipient_restrictions =reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'
[root@server.claudely.net ~]#
[root@server.claudely.net ~]#
```

The right window is mostly empty, showing only the title bar.

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.

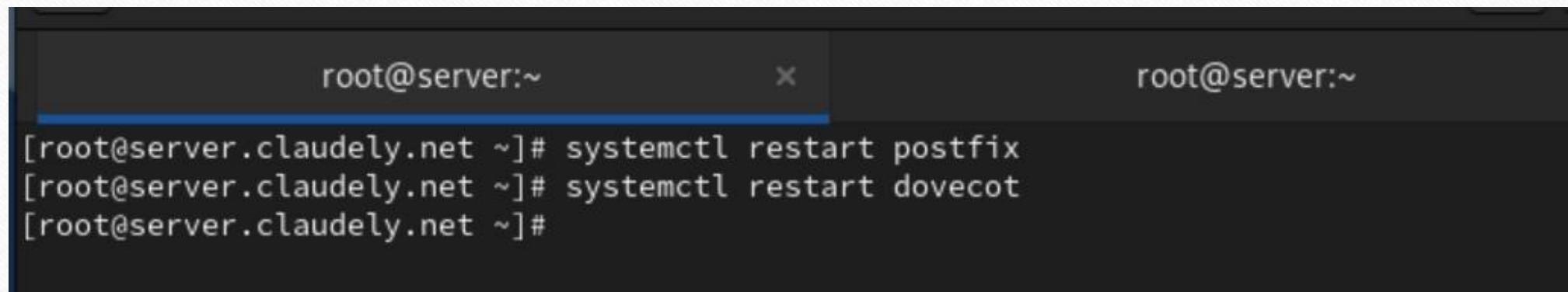
Настройка SMTP-аутентификации

```
#  
# 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.

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

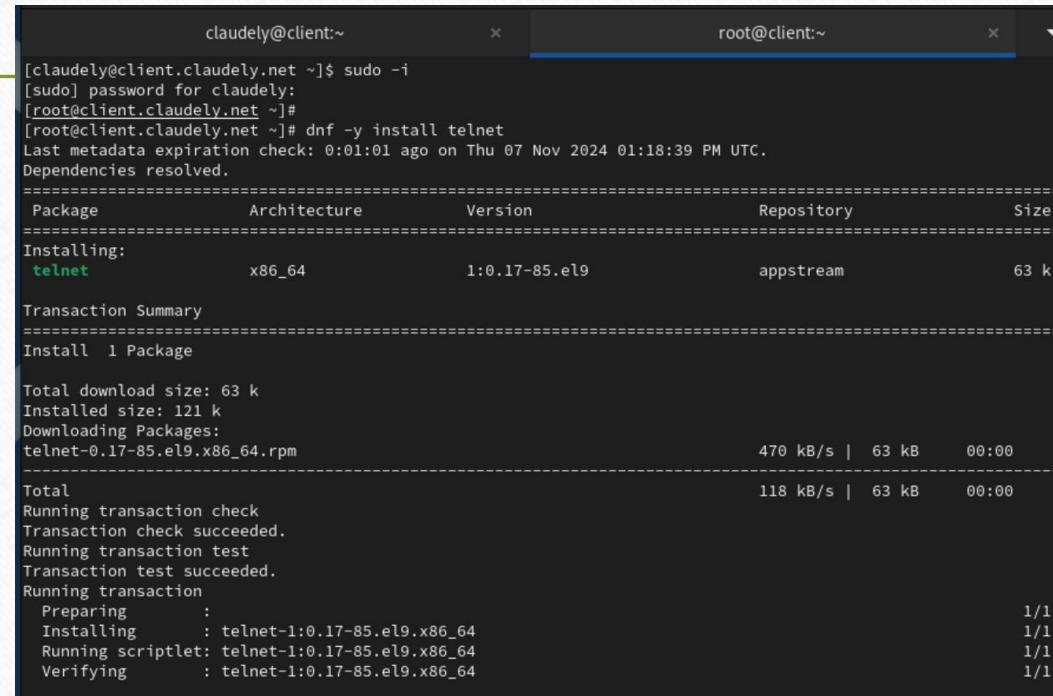
Настройка SMTP-аутентификации



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

Рис. 2.4. Перезапуск Postfix и Dovecot.

Настройка SMTP-аутентификации



```
[claudely@client.claudely.net ~]$ sudo -i
[sudo] password for claudely:
[root@client.claudely.net ~]#
[root@client.claudely.net ~]# dnf -y install telnet
Last metadata expiration check: 0:01:01 ago on Thu 07 Nov 2024 01:18:39 PM UTC.
Dependencies resolved.
=====
 Package           Architecture   Version      Repository    Size
=====
 Installing:
  telnet           x86_64        1:0.17-85.el9   appstream   63 k

Transaction Summary
=====
 Install 1 Package

Total download size: 63 k
Installed size: 121 k
Downloading Packages:
telnet-0.17-85.el9.x86_64.rpm
470 kB/s | 63 kB  00:00
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : telnet-1:0.17-85.el9.x86_64 1/1
Running scriptlet: telnet-1:0.17-85.el9.x86_64 1/1
Verifying  : telnet-1:0.17-85.el9.x86_64 1/1
```

Рис. 2.5. Установка на клиенте telnet.

Настройка SMTP-аутентификации

```
axNlcm5nbWUAdxNlcm5nbWUAcGFZc3dvcmQ=
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# printf 'claudely\x00claudely\x0001072001Ng' | base64
Y2xhdWRlbHkAY2xhdWRlbHkAMDEwNzIwMDF0Zw==
[root@server.claudely.net ~]# █
```

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/smtp
# -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_unknown_recipient_domain,permit_sasl_authenticated,reject
# -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
#628     inet  n       -       n       -       -           amavisd
```

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 dhcpcv6 dhcpcv6-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 gpfdist grafana gre high-availability http
http3 https ident imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins
kadmin kdeconnect kerberos kibana klogind 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 ntp-nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmcon
sole plex pmproxy pmwebapi pop3 pop3s postgresql privoxy prometheus prom
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 smtsp snmp snmpfsm snmpfsm-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 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 wsman 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 ~]#
```

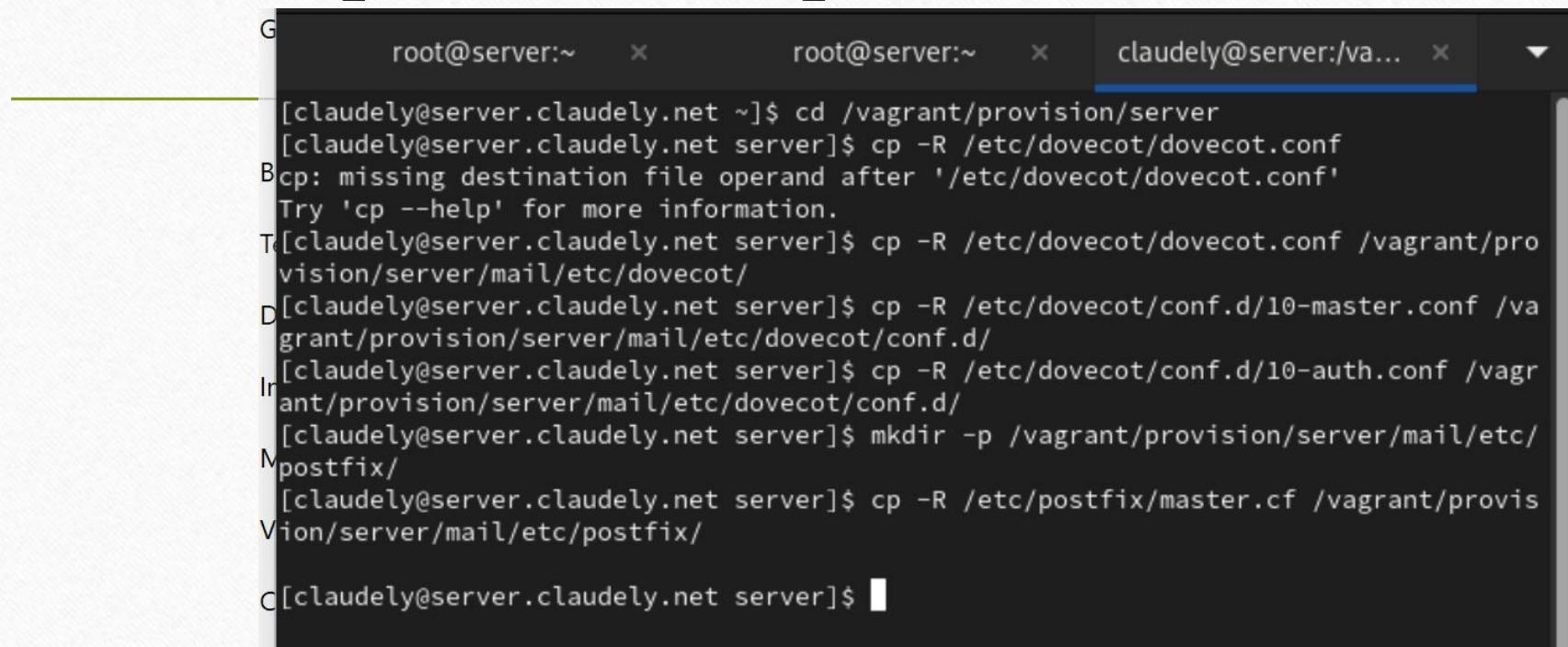
Рис. 3.3. Настройка межсетевого экрана, разрешив работать службе smtp-submission.

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



The screenshot shows a terminal window with three tabs open:

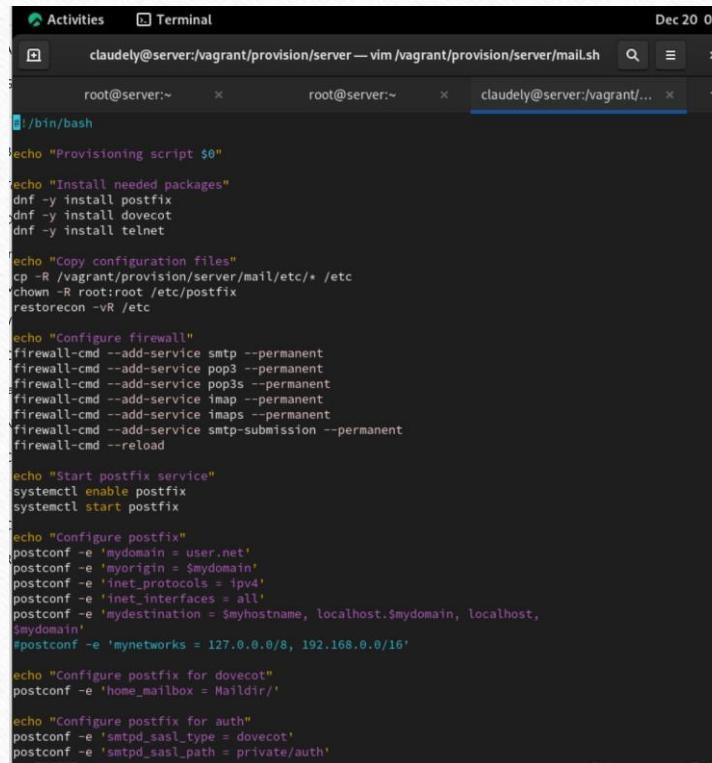
- Tab 1: root@server:~
- Tab 2: root@server:~
- Tab 3: claudely@server:/va... (highlighted)

The session in Tab 3 shows the following command-line history:

```
[claudely@server.claudely.net ~]$ cd /vagrant/provision/server
[claudely@server.claudely.net server]$ cp -R /etc/dovecot/dovecot.conf
Bcp: missing destination file operand after '/etc/dovecot/dovecot.conf'
Try 'cp --help' for more information.
T[claudely@server.claudely.net server]$ cp -R /etc/dovecot/dovecot.conf /vagrant/pro
vision/server/mail/etc/dovecot/
D[claudely@server.claudely.net server]$ cp -R /etc/dovecot/conf.d/10-master.conf /va
grant/provision/server/mail/etc/dovecot/conf.d/
I[claudely@server.claudely.net server]$ cp -R /etc/dovecot/conf.d/10-auth.conf /vagr
ant/provision/server/mail/etc/dovecot/conf.d/
[claudely@server.claudely.net server]$ mkdir -p /vagrant/provision/server/mail/etc/
Mpostfix/
[claudely@server.claudely.net server]$ cp -R /etc/postfix/master.cf /vagrant/provis
ion/server/mail/etc/postfix/
V[claudely@server.claudely.net server]$
```

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



The screenshot shows a terminal window titled "Terminal" with three tabs: "root@server:~" (inactive), "root@server:~" (inactive), and "claudely@server:/vagrant/...". The current tab displays a shell script named "mail.sh" with the following content:

```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install postfix
dnf -y install dovecot
dnf -y install telnet

echo "Copy configuration files"
cp -R /vagrant/provision/server/mail/etc/* /etc
chown -R root:root /etc/postfix
restorecon -vR /etc

echo "Configure firewall"
firewall-cmd --add-service smtp --permanent
firewall-cmd --add-service pop3 --permanent
firewall-cmd --add-service pop3s --permanent
firewall-cmd --add-service imap --permanent
firewall-cmd --add-service imaps --permanent
firewall-cmd --add-service smtp-submission --permanent
firewall-cmd --reload

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

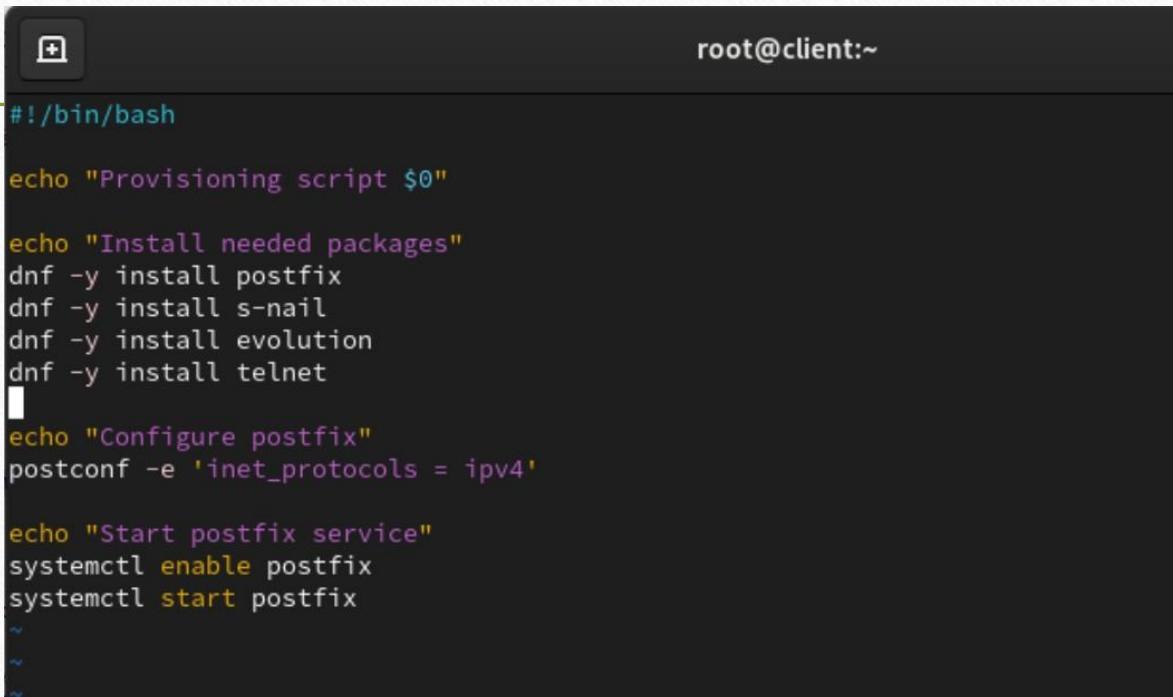
echo "Configure postfix"
postconf -e 'mydomain = user.net'
postconf -e 'myorigin = $mydomain'
postconf -e 'inet_protocols = ipv4'
postconf -e 'inet_interfaces = all'
postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost,
$mydomain'
#postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'

echo "Configure postfix for dovecot"
postconf -e 'home_mailbox = Maildir/'

echo "Configure postfix for auth"
postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'
```

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



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there is a small icon of a square with a plus sign, followed by the text "root@client:~". Below this, the terminal prompt is shown. The content of the terminal is a shell script named "mail.sh". The script starts with "#!/bin/bash" and contains several commands to install packages (postfix, s-nail, evolution, telnet) and configure postfix by adding "inet_protocols = ipv4" to its configuration file. It also starts the postfix service using systemctl. The script ends with three tilde characters (~).

```
#!/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!