

Отчет по лабораторной работе №10

Расширенные настройки SMTP-сервера

Галацан Николай, НПИбд-01-22

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
2.1	Настройка LMTP в Dovecot	5
2.2	Настройка SMTP-аутентификации	8
2.3	Настройка SMTP over TLS	10
2.4	Внесение изменений в настройки внутреннего окружения виртуальной машины	14
3	Выводы	16
4	Ответы на контрольные вопросы	17

Список иллюстраций

2.1	Редактирование файла /etc/dovecot/dovecot.conf	5
2.2	Редактирование файла /etc/dovecot/conf.d/10-master.conf	6
2.3	Редактирование файла /etc/dovecot/conf.d/10-auth.conf	7
2.4	Просмотр мониторинга почтовой службы на сервере	7
2.5	Просмотр почты	8
2.6	Редактирование файла /etc/dovecot/conf.d/10-master.conf	8
2.7	Изменение конфигурации Postfix	9
2.8	Редактирование файла /etc/postfix/master.cf для проверки аутентификации	9
2.9	Получение строки для аутентификации на клиенте, подключение к SMTP-серверу через telnet, проверка аутентификации	10
2.10	Конфигурации Postfix для настройки TLS	11
2.11	Изменение конфигураций для запуска SMTP-сервера на 587-порту	11
2.12	Настройка межсетевого экрана и перезапуск Postfix	12
2.13	Проверка подключения и аутентификации по telnet на клиенте	12
2.14	Изменение настроек учетной записи в Evolution	13
2.15	Проверка доставки письма в Evolution	13
2.16	Проверка почтового ящика на сервере	14
2.17	Редактирование mail.sh на сервере	15
2.18	Редактирование mail.sh на клиенте	15

1 Цель работы

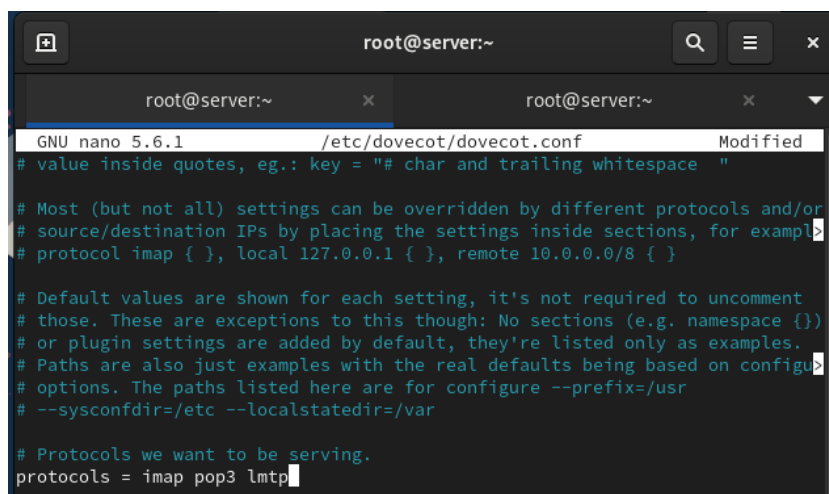
Приобретение практических навыков по конфигурированию SMTP-сервера в части настройки аутентификации.

2 Выполнение лабораторной работы

2.1 Настройка LMTP в Dovecot

Запускаю VM через рабочий каталог. На VM server вхожу под собственным пользователем и перехожу в режим суперпользователя. В доп. терминале запускаю мониторинг работы почтовой службы.

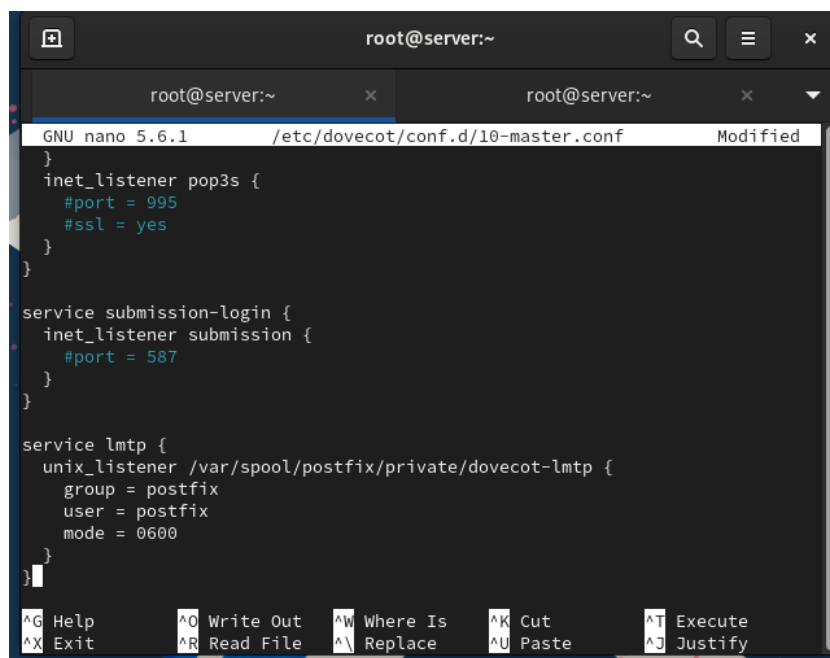
В конфигурационном файле `/etc/dovecot/dovecot.conf` добавляю в список почтовых протоколов `lmtp` (рис. 2.1).



```
root@server:~  
GNU nano 5.6.1 /etc/dovecot/dovecot.conf Modified  
# 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 configuration  
# 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. 2.1: Редактирование файла `/etc/dovecot/dovecot.conf`

В конфигурационном файле `/etc/dovecot/conf.d/10-master.conf` настраиваю сервис `lmtp` (рис. 2.2)



```
GNU nano 5.6.1 /etc/dovecot/conf.d/10-master.conf Modified
}
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
  }
}
```

Рис. 2.2: Редактирование файла /etc/dovecot/conf.d/10-master.conf

Переопределяю в Postfix с помощью передачу сообщений не напрямую, а через заданный unix-сокеты:

```
postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'
```

В конфигурационном файле /etc/dovecot/conf.d/10-auth.conf задаю формат имени пользователя для аутентификации в форме логина пользователя без указания домена (рис. 2.3)

Просматриваю почтовый ящик пользователя (рис. 2.5).

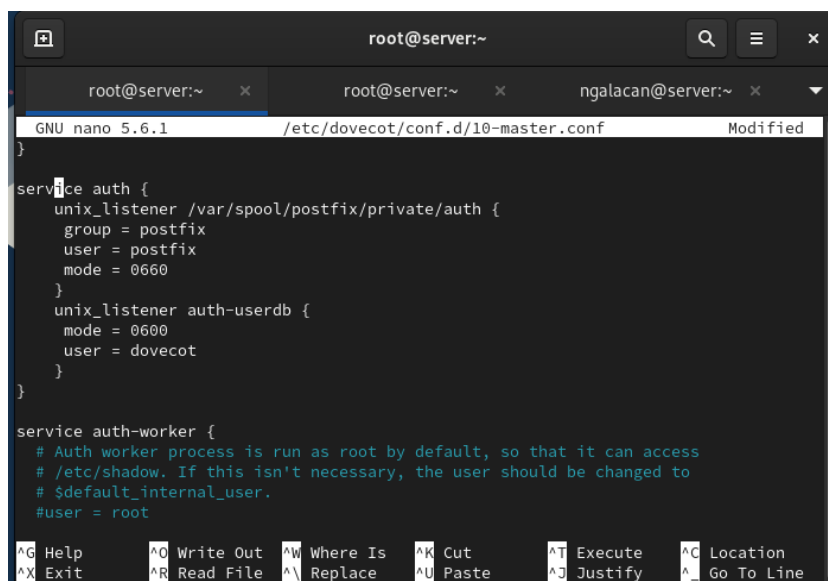
```
[ngalacan@server.ngalacan.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.22.  Type '?' for help
/home/ngalacan/Maildir: 3 messages 1 new
 1 ngalacan@ngalacan.ne 2024-10-09 17:01 14/444 "test"
 2 ngalacan 2024-10-16 13:49 18/648 "test3"
 *N 3 ngalacan@client.ngal 2024-10-16 15:54 21/833 "LMTP-test"
&
```

Рис. 2.5: Просмотр почты

Письмо доставлено.

2.2 Настройка SMTP-аутентификации

В конфигурационном файле `/etc/dovecot/conf.d/10-master.conf` определяю службу аутентификации пользователей (рис. 2.6).

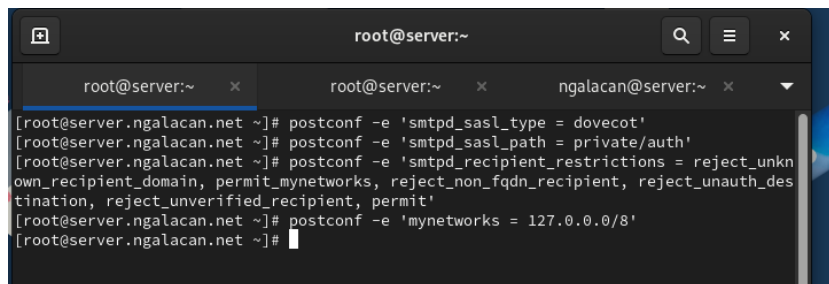


```
root@server:~
GNU nano 5.6.1 /etc/dovecot/conf.d/10-master.conf Modified
}
service auth {
  unix_listener /var/spool/postfix/private/auth {
    group = postfix
    user = postfix
    mode = 0660
  }
  unix_listener auth-userdb {
    mode = 0600
    user = dovecot
  }
}

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
}
```

Рис. 2.6: Редактирование файла `/etc/dovecot/conf.d/10-master.conf`

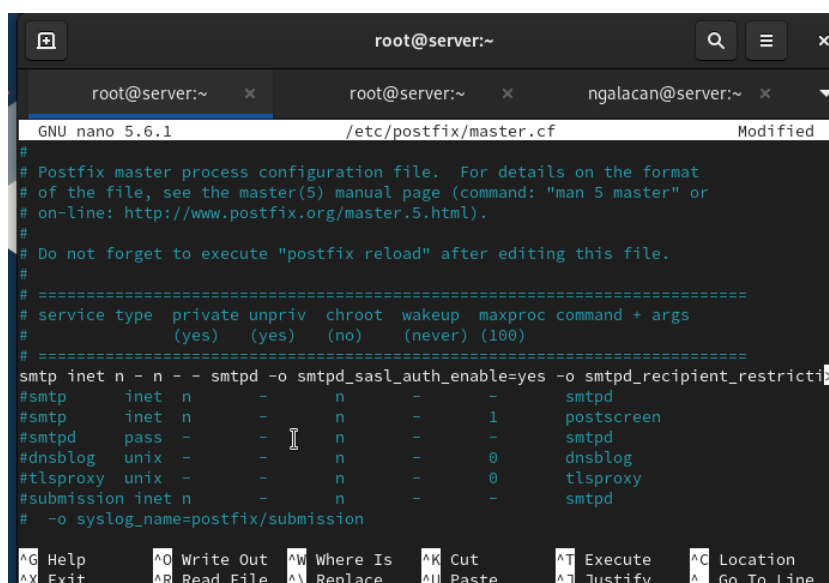
Изменяю конфигурацию Postfix, задав тип аутентификации, путь к unix-сокету, произведя настройку для приема почты (рис. 2.7).



```
root@server:~  
[root@server.ngalacan.net ~]# postconf -e 'smtpd_sasl_type = dovecot'  
[root@server.ngalacan.net ~]# postconf -e 'smtpd_sasl_path = private/auth'  
[root@server.ngalacan.net ~]# postconf -e 'smtpd_recipient_restrictions = reject_unkn  
own_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_des  
tination, reject_unverified_recipient, permit'  
[root@server.ngalacan.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'  
[root@server.ngalacan.net ~]#
```

Рис. 2.7: Изменение конфигурации Postfix

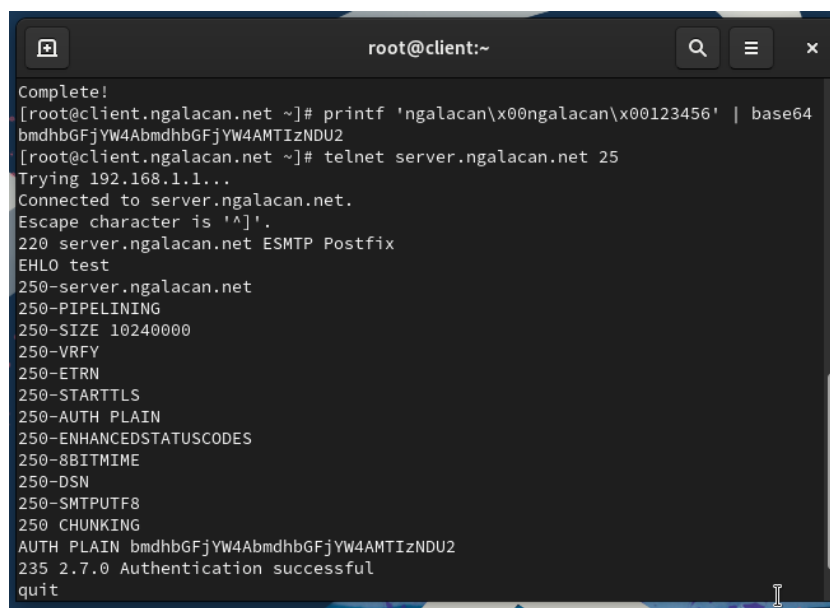
В файле `/etc/postfix/master.cf` изменяю запись для проверки работы аутен-
тификации (рис. 2.8).



```
GNU nano 5.6.1 /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 -o smtpd_sasl_auth_enable=yes -o smtpd_recipient_restricti  
#smtp inet n - n - - smtpd  
#smtp inet n - n - 1 postscreen  
#smtpd pass - - n - - smtpd  
#dnsblog unix - - n - 0 dnsblog  
#tlsproxy unix - - n - 0 tlsproxy  
#submission inet n - n - - smtpd  
# -o syslog_name=postfix/submission  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^_ Replace ^U Paste ^J Justify ^_ Go To Line
```

Рис. 2.8: Редактирование файла `/etc/postfix/master.cf` для проверки аутентифика-
ции

Перезапускаю Postfix и Dovecot. На клиенте устанавливаю telnet. Получаю
строку для аутентификации, подключаюсь к SMTP-серверу через telnet. Тести-
рую соединение и проверяю аутентификацию (успешно) и завершаю сессию (рис.
2.9).



```
Complete!
[root@client.ngalacan.net ~]# printf 'ngalacan\x00ngalacan\x00123456' | base64
bmdhbgGFjYW4AbmdhbgGFjYW4AMTIzNDU2
[root@client.ngalacan.net ~]# telnet server.ngalacan.net 25
Trying 192.168.1.1...
Connected to server.ngalacan.net.
Escape character is '^]'.
220 server.ngalacan.net ESMTP Postfix
EHLO test
250-server.ngalacan.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN bmdhbgGFjYW4AbmdhbgGFjYW4AMTIzNDU2
235 2.7.0 Authentication successful
quit
```

Рис. 2.9: Получение строки для аутентификации на клиенте, подключение к SMTP-серверу через telnet, проверка аутентификации

2.3 Настройка SMTP over TLS

Настраиваю на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно копирую необходимые файлы сертификата и ключа из каталога `/etc/pki/dovecot` в каталог `/etc/pki/tls/` в соответствующие подкаталоги, затем конфигурирую Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности (рис. 2.10).

```

root@server:~
root@server.ngalacan.net ~]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs/
root@server.ngalacan.net ~]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
root@server.ngalacan.net ~]# postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
root@server.ngalacan.net ~]# postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
root@server.ngalacan.net ~]# postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
root@server.ngalacan.net ~]# postconf -e 'smtpd_tls_security_level = may'
> ^C
root@server.ngalacan.net ~]# postconf -e 'smtpd_tls_security_level = may'
root@server.ngalacan.net ~]# postconf -e 'smtpd_tls_security_level = may'
root@server.ngalacan.net ~]#

```

Рис. 2.10: Конфигурации Postfix для настройки TLS

Для того чтобы запустить SMTP-сервер на 587-м порту, заменяю запись в файле `/etc/postfix/master.cf` (рис. 2.11).

```

GNU nano 5.6.1 /etc/postfix/master.cf Modified
# 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 - 1 postscreen
#smtpd pass - - n - - smtpd
#dnsblog unix - - n - 0 dnsblog
#tlsproxy unix - - n - 0 tlsproxy
#submission inet n - n - smtpd -o smtpd_tls_security_level=encrypt -o smtpd_sasl_auth_enable=yes
#submission inet n - n - - smtpd
# -o syslog_name=postfix/submission
# -o smtpd_tls_security_level=encrypt
# -o smtpd_sasl_auth_enable=yes

```

Рис. 2.11: Изменение конфигураций для запуска SMTP-сервера на 587-порту

Настраиваю межсетевой экран и перезапускаю Postfix (рис. 2.12)

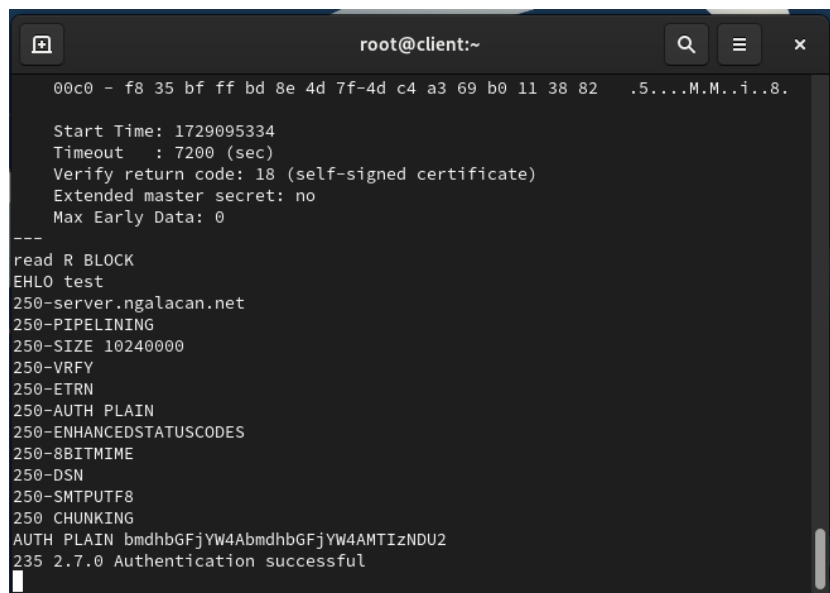
```
[root@server.ngalacan.net ~]# firewall-cmd --add-service=smtp-submission
success
[root@server.ngalacan.net ~]# firewall-cmd --add-service=smtp-submission --permanent
success
[root@server.ngalacan.net ~]# firewall-cmd --reload
success
[root@server.ngalacan.net ~]# systemctl restart postfix
bash: systemctl: command not found...
[root@server.ngalacan.net ~]# systemctl restart postfix
[root@server.ngalacan.net ~]#
```

Рис. 2.12: Настройка межсетевого экрана и перезапуск Postfix

На клиенте подключаюсь к SMTP-серверу через 587-й порт посредством openssl

```
openssl s_client -starttls smtp -crlf -connect server.ngalacan.net:587
```

Тестирую подключение. Проверяю аутентификацию (успешно) (рис. 2.13).



```
root@client:~
00c0 - f8 35 bf ff bd 8e 4d 7f-4d c4 a3 69 b0 11 38 82 .5....M.M..i..8.

Start Time: 1729095334
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
EHLO test
250-server.ngalacan.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN bmdhbgfjYW4AbmdhbGFjYW4AMTIzNDU2
235 2.7.0 Authentication successful
```

Рис. 2.13: Проверка подключения и аутентификации по telnet на клиенте

Проверяю корректность отправки почтовых сообщений с клиента посредством почтового клиента Evolution, предварительно скорректировав настройки учётной записи, а именно для SMTP-сервера указав порт 587, STARTTLS и обычный пароль (рис. 2.14). Письмо доставлено (рис. 2.15).

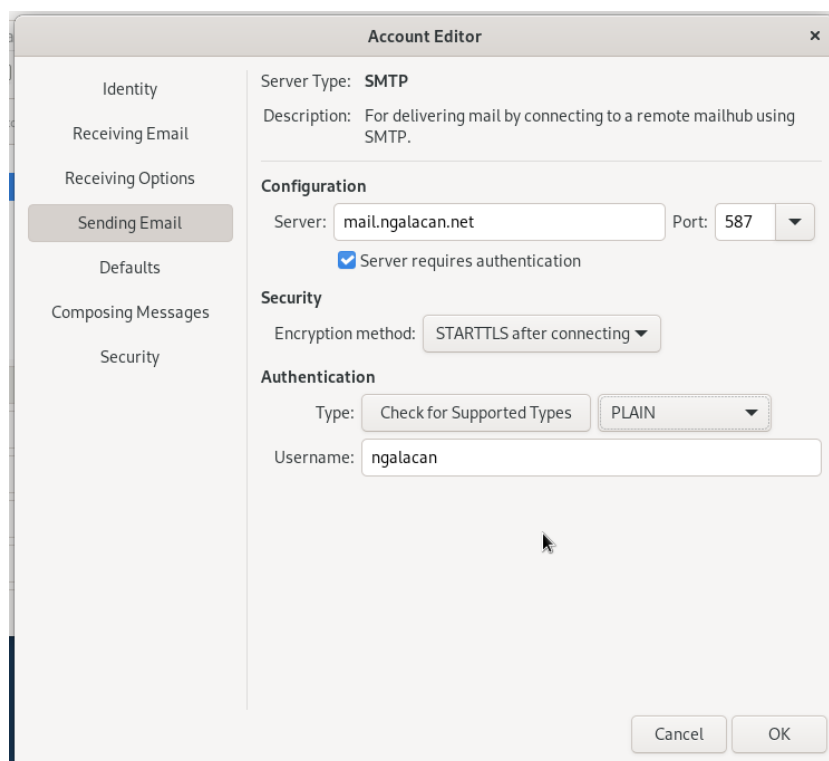


Рис. 2.14: Изменение настроек учетной записи в Evolution

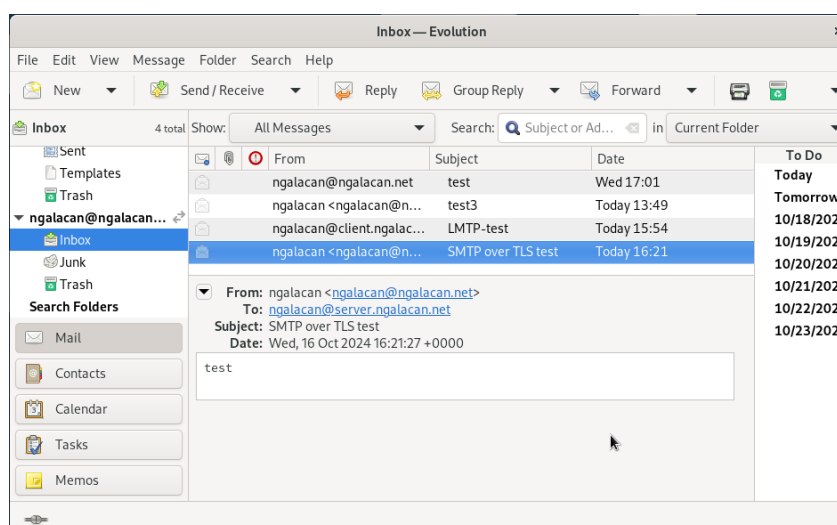
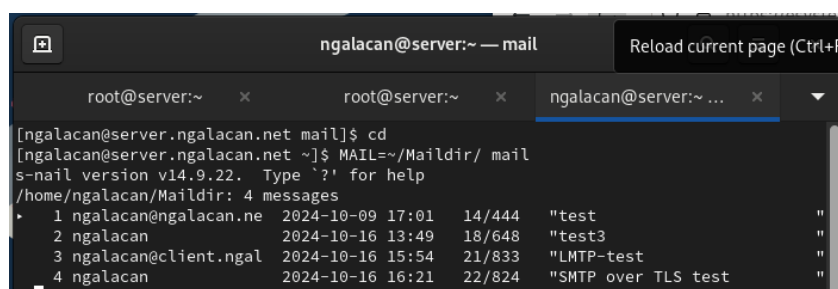


Рис. 2.15: Проверка доставки письма в Evolution

Также на сервере проверяю почтовый ящик (рис. 2.16).



```
ngalacan@server:~ — mail
root@server:~ x root@server:~ x ngalacan@server:~ ... x
[ngalacan@server.ngalacan.net mail]$ cd
[ngalacan@server.ngalacan.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/ngalacan/Maildir: 4 messages
┌ 1 ngalacan@ngalacan.ne 2024-10-09 17:01 14/444 "test"
└ 2 ngalacan 2024-10-16 13:49 18/648 "test3"
  3 ngalacan@client.ngal 2024-10-16 15:54 21/833 "LMTP-test"
  4 ngalacan 2024-10-16 16:21 22/824 "SMTP over TLS test"
```

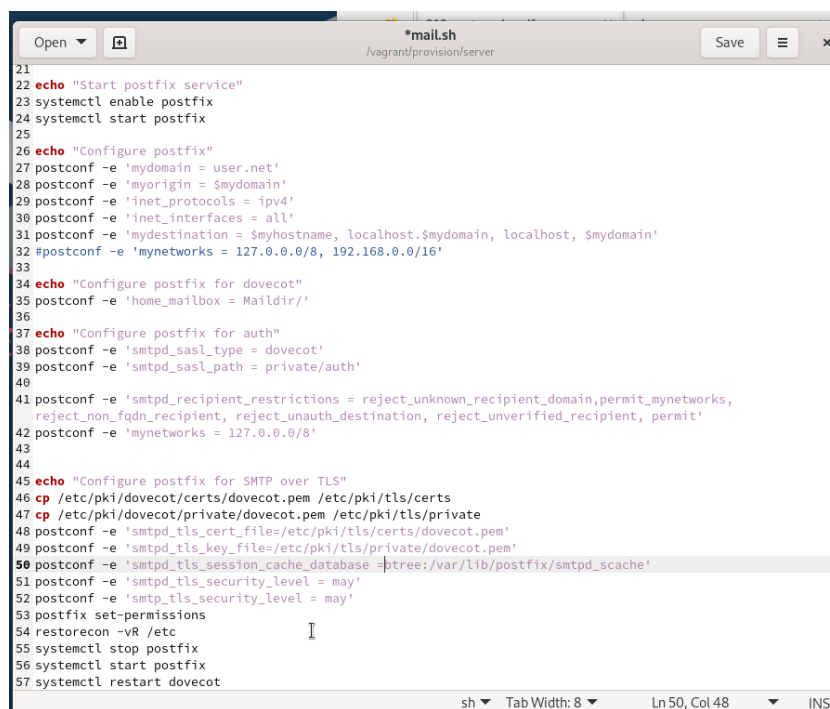
Рис. 2.16: Проверка почтового ящика на сервере

2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На VM server перехожу в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/` и копирую в соответствующие каталоги конфигурационные файлы:

```
cd /vagrant/provision/server
cp -R /etc/dovecot/dovecot.conf
    ↪ /vagrant/provision/server/mail/etc/dovecot/
cp -R /etc/dovecot/conf.d/10-master.conf
    ↪ /vagrant/provision/server/mail/etc/dovecot/conf.d/
cp -R /etc/dovecot/conf.d/10-auth.conf
    ↪ /vagrant/provision/server/mail/etc/dovecot/conf.d/
mkdir -p /vagrant/provision/server/mail/etc/postfix/
cp -R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postfix/
```

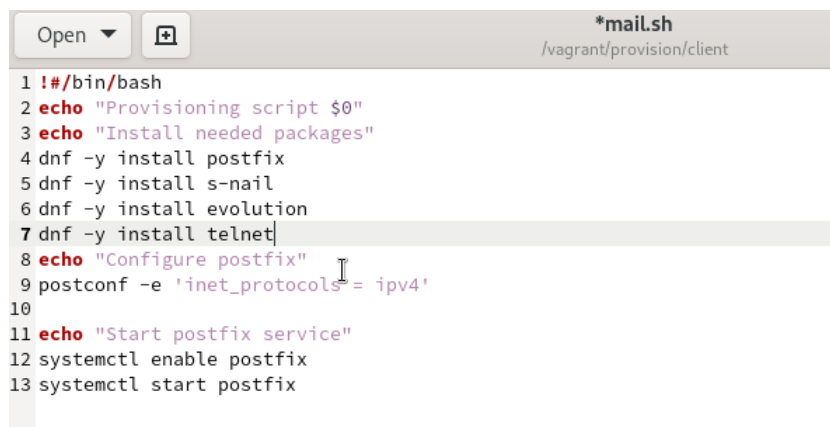
Вношу изменения в файл `/vagrant/provision/server/mail.sh` (рис. 2.17).

A screenshot of a terminal window titled '*mail.sh' with the path '/vagrant/provision/server'. The window shows a script for configuring postfix and dovecot. The script includes commands for enabling and starting postfix, configuring postfix with various options like mydomain, myorigin, inet_protocols, inet_interfaces, mydestination, mynetworks, home_mailbox, smtpd_sasl_type, and smtpd_sasl_path. It also includes commands for configuring postfix for SMTP over TLS, copying certificates, and setting permissions. The script ends with commands to stop and start postfix, and restart dovecot. The cursor is at the end of line 57.

```
21
22 echo "Start postfix service"
23 systemctl enable postfix
24 systemctl start postfix
25
26 echo "Configure postfix"
27 postconf -e 'mydomain = user.net'
28 postconf -e 'myorigin = $mydomain'
29 postconf -e 'inet_protocols = ipv4'
30 postconf -e 'inet_interfaces = all'
31 postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain'
32 #postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'
33
34 echo "Configure postfix for dovecot"
35 postconf -e 'home_mailbox = Maildir/'
36
37 echo "Configure postfix for auth"
38 postconf -e 'smtpd_sasl_type = dovecot'
39 postconf -e 'smtpd_sasl_path = private/auth'
40
41 postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks,
reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'
42 postconf -e 'mynetworks = 127.0.0.0/8'
43
44
45 echo "Configure postfix for SMTP over TLS"
46 cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
47 cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
48 postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
49 postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
50 postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
51 postconf -e 'smtpd_tls_security_level = may'
52 postconf -e 'smtpd_tls_security_level = may'
53 postfix set-permissions
54 restorecon -vR /etc
55 systemctl stop postfix
56 systemctl start postfix
57 systemctl restart dovecot
```

Рис. 2.17: Редактирование mail.sh на сервере

На VM client перехожу в каталог для внесения изменений в настройки внутреннего окружения и редактирую скрипт /vagrant/provision/client/mail.sh (рис. 2.18).

A screenshot of a terminal window titled '*mail.sh' with the path '/vagrant/provision/client'. The window shows a script for provisioning the client environment. The script includes commands for installing postfix, s-nail, evolution, and telnet. It also includes commands for configuring postfix with inet_protocols = ipv4 and starting the postfix service. The cursor is at the end of line 13.

```
1 !#/bin/bash
2 echo "Provisioning script $0"
3 echo "Install needed packages"
4 dnf -y install postfix
5 dnf -y install s-nail
6 dnf -y install evolution
7 dnf -y install telnet
8 echo "Configure postfix"
9 postconf -e 'inet_protocols = ipv4'
10
11 echo "Start postfix service"
12 systemctl enable postfix
13 systemctl start postfix
```

Рис. 2.18: Редактирование mail.sh на клиенте

3 Выводы

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

4 Ответы на контрольные вопросы

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

- `auth_username_format = %Lu@d`

2. 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.

3. 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.