

# Отчёт по лабораторной работе 10

## Расширенные настройки SMTP-сервера.

Цвелев С.А. НПИбд-02-22

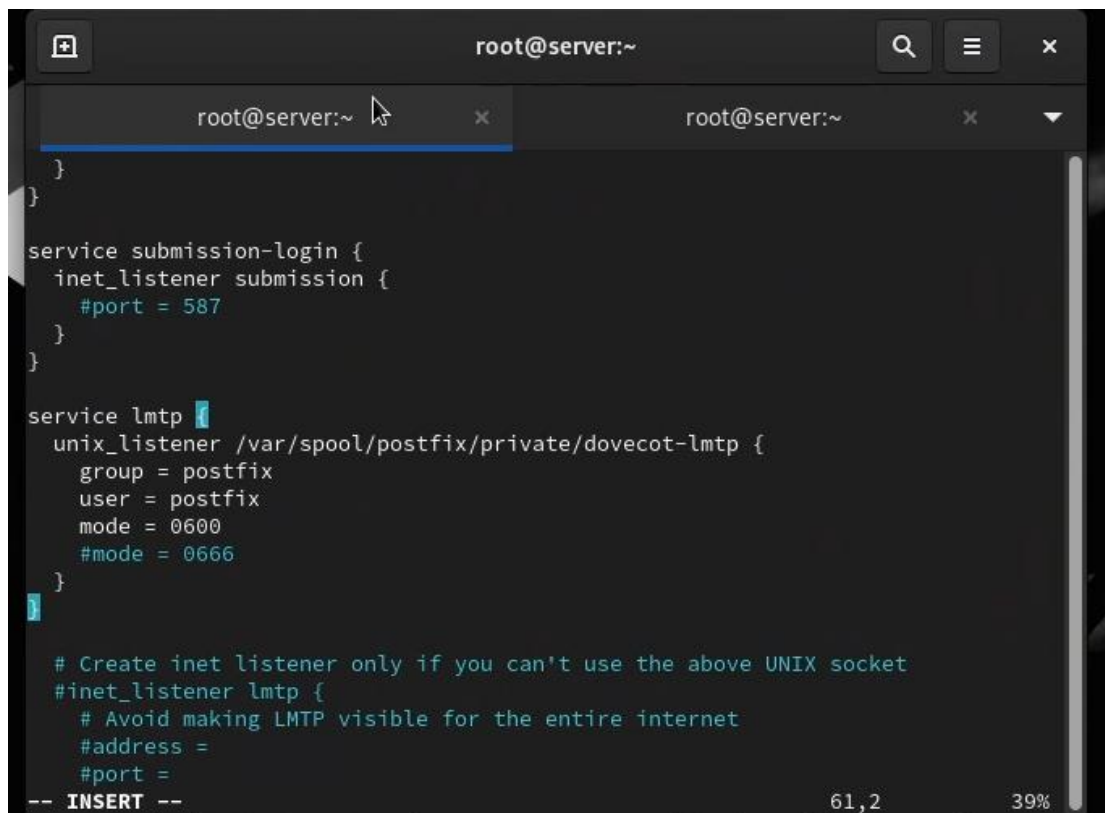
### Содержание

#### 1 Цель работы

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

#### 2 Ход работы

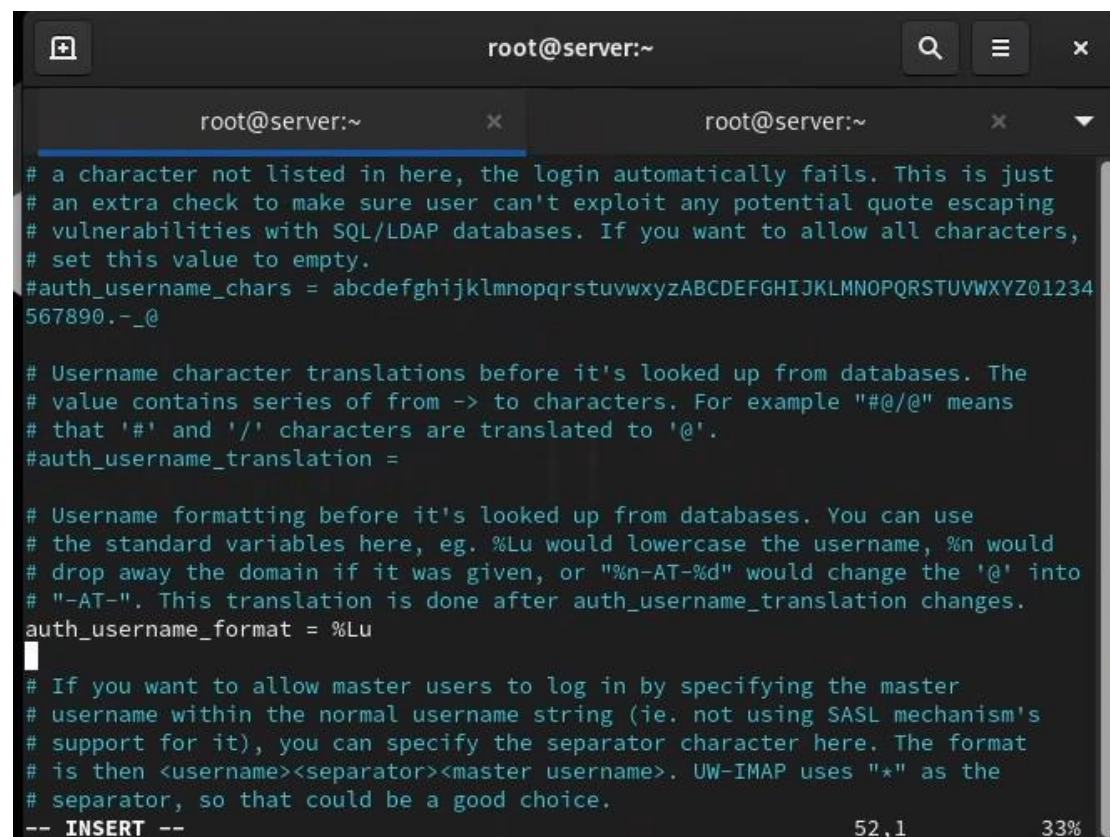
Запускаем машину server и входим в режим суперпользователя. Запускаем в отдельном терминале мониторинг работы почтовой службы. Добавляем в список разрешенных протоколов Dovecot LMTP. Настраиваем этот сервис для связи с Postfix.



```
root@server:~  
}  
}  
service submission-login {  
  inet_listener submission {  
    #port = 587  
  }  
}  
  
service lmtp {  
  unix_listener /var/spool/postfix/private/dovecot-lmtp {  
    group = postfix  
    user = postfix  
    mode = 0600  
    #mode = 0666  
  }  
}  
  
# 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 =  
-- INSERT --
```

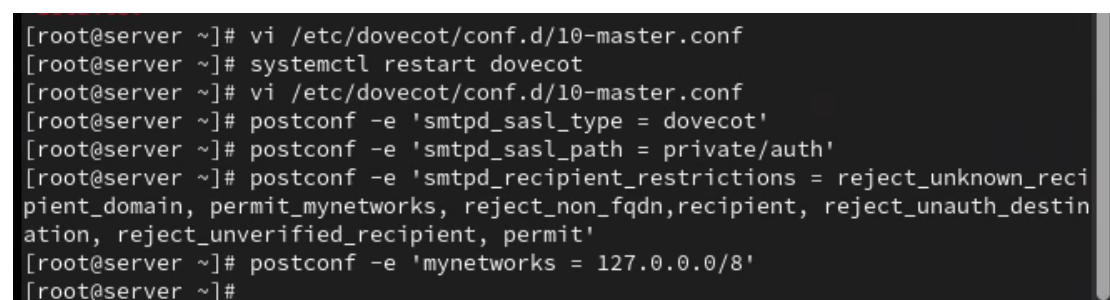
61,2 39%

Переопределяем передачу сообщений через заданный unix-сокеты. Задаем формат имени пользователя без указания домена. Перезапускаем службы и отправляем себе письмо с клиента.



```
root@server:~  
# a character not listed in here, the login automatically fails. This is just  
# an extra check to make sure user can't exploit any potential quote escaping  
# vulnerabilities with SQL/LDAP databases. If you want to allow all characters,  
# set this value to empty.  
#auth_username_chars = abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234  
567890.-_@  
  
# 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 = %Lu  
  
# If you want to allow master users to log in by specifying the master  
# username within the normal username string (ie. not using SASL mechanism's  
# support for it), you can specify the separator character here. The format  
# is then <username><separator><master username>. UW-IMAP uses "*" as the  
# separator, so that could be a good choice.  
-- INSERT --
```

Определяем службу аутентификации пользователей. Задаем тип аутентификации SASL для smtpd и путь к соответствующему сокету. Настраиваем прием почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной сети. Ограничиваем прием почты только локальным адресом SMTP-сервера сети. Временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Перезапускаем службы.



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

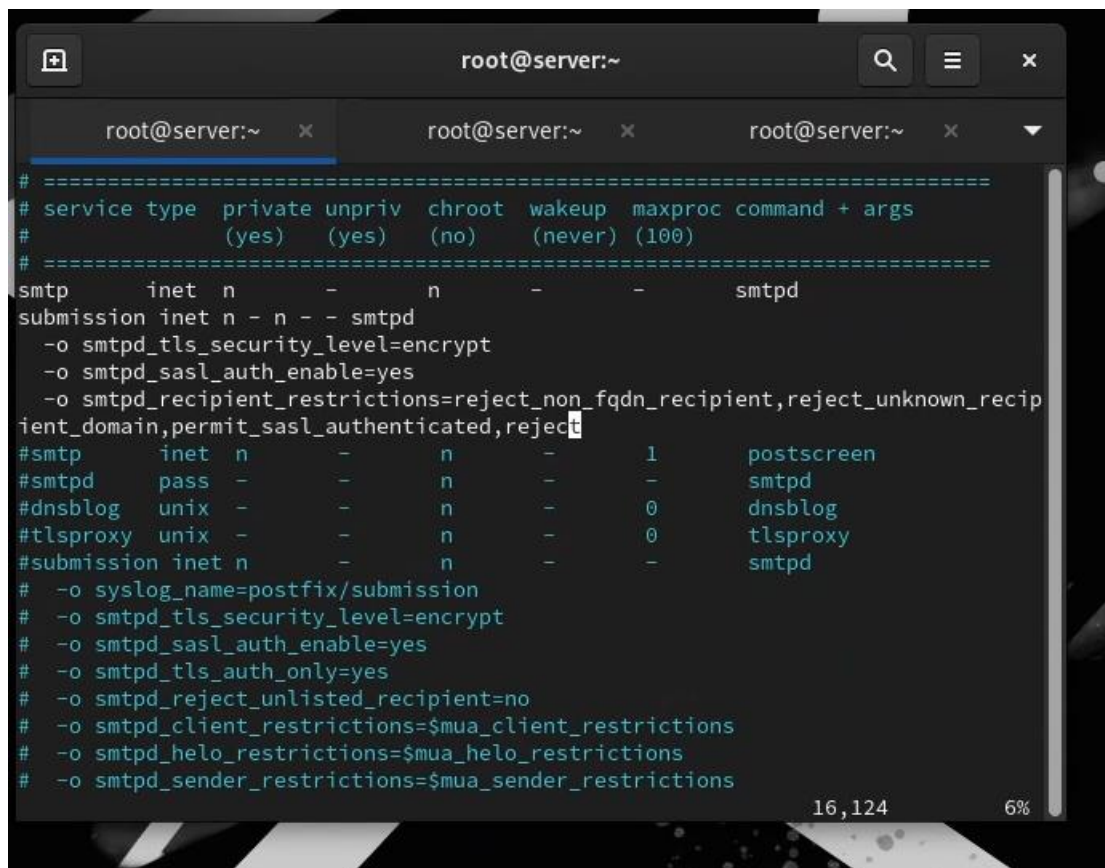
Устанавливаем telnet на клиенте. Получаем строку для аутентификации и подключаемся через telnet к SMTP-серверу.

```
root@client:~  
Downloading Packages:  
telnet-0.17-85.el9.x86_64.rpm                890 kB/s | 63 kB    00:00  
-----  
Total                                      151 kB/s | 63 kB    00:00  
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  
  
Installed:  
  telnet-1:0.17-85.el9.x86_64  
  
Complete!  
[root@client ~]# printf 'sacvelev\x00sacvelev\x00123456' | base64  
c2FjdmdVsZXYAc2FjdmdVsZXYAMTIzNDU2  
[root@client ~]# telnet server.sacvelev.net 25
```

Настраиваем TLS, воспользовавшись временным сертификатом Dovecot.  
Копируем необходимые файлы сертификата и ключа в другие каталоги.  
Настраиваем postfix, указав пути к сертификату и ключу, а также к каталогу TLS-сессий.

```
root@server:~  
root@server:~ x root@server:~ x root@server:~ x  
details.  
[root@server ~]# vi /etc/dovecot/conf.d/10-master.conf  
[root@server ~]# systemctl restart dovecot  
[root@server ~]# vi /etc/dovecot/conf.d/10-master.conf  
[root@server ~]# postconf -e 'smtpd_sasl_type = dovecot'  
[root@server ~]# postconf -e 'smtpd_sasl_path = private/auth'  
[root@server ~]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'  
[root@server ~]# postconf -e 'mynetworks = 127.0.0.0/8'  
[root@server ~]# vi /etc/postfix/master.cf  
[root@server ~]# systemctl restart postfix  
[root@server ~]# systemctl restart dovecot  
[root@server ~]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs  
[root@server ~]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private  
[root@server ~]# postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'  
[root@server ~]# postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'  
[root@server ~]# postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'  
[root@server ~]# postconf -e 'smtpd_tls_security_level = may'  
[root@server ~]# postconf -e 'smtpd_tls_security_level = may'
```

Для запуска SMTP-сервера на 587-м порту, меняем строки в файле master.cf.  
Настраиваем межсетевой экран, восстанавливаем контекст безопасности и перезапускаем службы.



```
# =====  
# service type private unpriv chroot wakeup maxproc command + args  
#               (yes)   (yes)   (no)   (never) (100)  
# =====  
smtp      inet  n       -       n       -       -       smtpd  
submission inet  n       -       n       -       -       smtpd  
  -o smtpd_tls_security_level=encrypt  
  -o smtpd_sasl_auth_enable=yes  
  -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recip  
  ient_domain,permit_sasl_authenticated,reject  
#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  
#  -o smtpd_tls_security_level=encrypt  
#  -o smtpd_sasl_auth_enable=yes  
#  -o smtpd_tls_auth_only=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
```

16,124 6%

### 3 Вывод

Мы приобрели навыки по конфигурированию SMTP-сервера в части настройки аутентификации.