Почтовый сервер с нуля

Разберем настройку на базе операционной системы (далее - ОС) Ubuntu 20.04.

> Все действия можно выполнять сразу под root, либо постоянно вначале каждой команды писать sudo и вводить пароль.

> Так же обращаю внимание, что в тексте будут строки, для внесения изменений в конфигурационные файлы. Удалять лишнее если я об этом не пишу, не нужно. Только редактируем и добавляем то что читаете.

Предварительная подготовка

Обновление ОС

```
apt update
```

```
apt upgrade
```

Важно переименовать сервер т.к. многие анти спам системы проверяют, обращение к серверу по имени

```
hostnamectl set-hostname mail.fellk.ru
```

Настройка синхронизации времени

```
apt install chrony
```

```
timedatectl set-timezone Europe/Moscow
```

```
systemctl enable chrony
```

Открываем порты с помощью iptables

```
iptables -I INPUT 1 -p tcp --match multiport --dports
25,110,143,465,587,993,995 -j ACCEPT
```

```
iptables -I INPUT 1 -p tcp --match multiport --dports 80,443 -j ACCEPT
```

Что бы сохранить правила делаем

```
apt install iptables-persistent
```

```
netfilter-persistent save
```

Настройка веб-сервера: Apache2 + PHP + MariaDB

Устанавливаем apache2 и включаем автозапуск

```
apt install apache2
```

```
systemctl enable apache2
```

Проверить работу сервера можно перейдя по ссылке http://10.0.1.18

Видите эту картинку?

Значит все супер, движемся дальше.

Устанавливаем php и php-fpm и делаем автозапуск

```
apt install php8.1 php8.1-fpm
```

```
systemctl enable php8.1-fpm
```

проверить версию можно так

```
php -v
```

Ставим доп.компоненты для php

```
apt install php8.1-mysql php8.1-mbstring php8.1-imap libapache2-mod-php8.1
```

Для применения перезапускаем

```
systemctl restart php8.1-fpm
```

Чтобы проверить работоспособность php создаем файл

```
nano /var/www/html/index.php
```

вписываем в файл строку

```
<?php phpinfo(); ?>
```

Проверить работу можно перейдя по ссылке http://10.0.1.18/index.php

Видите эту картинку?

20230925-072123.png_nolink

Значит все супер, движемся дальше.

Устанавливаем сервер баз данных и делаем автозапуск

```
apt install mariadb-server
```

```
systemctl enable mariadb
```

Задаем пароль для пользователя root:

```
mysqladmin -u root password
```

Установка и настройка PostfixAdmin

Скачиваем PostfixAdmin

```
wget https://sourceforge.net/projects/postfixadmin/files/latest/download -O
postfixadmin.tar.gz
```

Создать каталог postfixadmin и распаковать в него архив

```
mkdir /var/www/html/postfixadmin
```

```
tar -C /var/www/html/postfixadmin -xvf postfixadmin.tar.gz --strip-components 1
```

Создать каталог templates_c внутри папки postfixadmin (нужен для запуска установки)

```
mkdir /var/www/html/postfixadmin/templates_c
```

Задаем права на каталог

```
chown -R www-data:www-data /var/www/html/postfixadmin
```

php-fpm по умолчанию, запускается от пользователя www-data

Создать базу данных postfix и учетную запись

```
mysql -u root -p
```

```
CREATE DATABASE fellk DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_general_ci;
```

```
GRANT ALL ON fellk.* TO 'fellk'@'localhost' IDENTIFIED BY 'Ваш пароль';
```

```
quit;
```

localhost разрешает подключение только с локального сервера.

Создаем конфигурационный файл postfixadmin

```
nano /var/www/html/postfixadmin/config.local.php
```

И добавляем туда

```
<?php

$CONF['configured'] = true;
$CONF['default_language'] = 'ru';
$CONF['database_password'] = 'password123456';
$CONF['emailcheck_resolve_domain']='NO';

?>
```

В браузере вводим адрес http://10.0.1.18/postfixadmin/public/setup.php

Задаем пароль установки и генерируем хэш

Вставить ее необходимо в файл в самый низ до закрывающей скобки

```
nano /var/www/html/postfixadmin/config.local.php
```

Перезагружаем страницу http://10.0.1.18/postfixadmin/public/setup.php — появится форма ввода пароля. Как вы могли понять, пароль вводите, который вводили на предыдущем шаге.

Будет выполнена установка PostfixAdmin. По итогу не должно быть никаких ошибок, но если вдруг они будут, то на экране будет видно чего не хватает системе и нужно будет просто доустановить.

После успешной установки на экране появится возможность завести суперпользователя

Setup password — пароль с предыдущего шага;

Админ — root@fellk.ru

Пароль — новый пароль для создаваемой учетной записи

Переходим в браузере на страницу http://10.0.1.18/postfixadmin/public/login.php

Вводим логин и пароль только что созданные и попадаем в панель управления.

Установка и настройка Postfix

Ставим программу и зависимости командой

```
apt install postfix postfix-mysql
```

В процессе появится окно «Postfix Configuration» — оставляем Internet Site: В следующем окне оставляем имя сервера и нажимаем Enter.

После установки создаем учетную запись, от которой мы будем работать с каталогом виртуальных почтовых ящиков

```
groupadd -g 1024 mail
```

```
useradd -d /mail -g 1024 -u 1024 mail -m
```

Задаем владельца

```
chown mail:mail /mail
```

Приводим строки к такому виду

В файле

```
nano /etc/postfix/main.cf
```

```
mydestination = localhost.$mydomain, localhost, localhost.localdomain
inet_protocols = ipv4
smtpd_tls_cert_file = /etc/ssl/mail/cert.pem
smtpd_tls_key_file = /etc/ssl/mail/cert.key
myhostname = mail.fellk.ru
```

smtpd_tls_cert_file — путь и названия сертификатов у вас могут отличаться.

smtpd_tls_key_file — путь и названия сертификатов у вас могут отличаться.

В конец этого же файла допишем следующее

```
virtual_mailbox_base = /mail
virtual_alias_maps = proxy:mysql:/etc/postfix/mysql_virtual_alias_maps.cf
virtual_mailbox_domains =
proxy:mysql:/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_maps =
proxy:mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_minimum_uid = 1024
virtual_uid_maps = static:1024
virtual_gid_maps = static:1024
virtual_transport = dovecot
dovecot_destination_recipient_limit = 1

smtpd_sasl_auth_enable = yes
smtpd_sasl_exceptions_networks = $mynetworks
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth

smtp_use_tls = yes
smtpd_use_tls = yes
smtpd_tls_auth_only = yes
smtpd_helo_required = yes
```

Создать файл с настройками обращения к базе с алиасами

```
nano /etc/postfix/mysql_virtual_alias_maps.cf
```

```
user = root

password = Ваш пароль

hosts = localhost

dbname = fellk

query = SELECT goto FROM alias WHERE address='%s' AND active = '1'
```

Создать файл с инструкцией получения данных по виртуальным доменам

```
nano /etc/postfix/mysql_virtual_domains_maps.cf
```

```
user = root

password = Ваш пароль

hosts = localhost

dbname = fellk

query = SELECT domain FROM domain WHERE domain='%u'
```

Файл с почтовыми ящиками

```
nano /etc/postfix/mysql_virtual_mailbox_maps.cf
```

```
user = root

password = Ваш пароль

hosts = localhost

dbname = fellk

query = SELECT CONCAT(domain,'/',maildir) FROM mailbox WHERE username='%s'
AND active = '1'
```

Дописать в конце в файле master.cf

```
nano /etc/postfix/master.cf
```

```
submission   inet  n  -  n  -  -  smtpd
  -o smtpd_tls_security_level=may
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=/var/spool/postfix/private/auth
  -o smtpd_sasl_security_options=noanonymous
  -o smtpd_sasl_local_domain=$myhostname
```

```
smtps   inet  n  -  n  -  -  smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject

dovecot   unix  -  n  n  -  -  pipe
  flags=DRhu user=mail:mail argv=/usr/lib/dovecot/deliver -d ${recipient}
```

Генерируем сертификаты безопасности. Либо приобретаем готовые у своего хостинг провайдера

Создаем папку

```
mkdir -p /etc/ssl/mail
```

SSL сертификат куплен у провайдера timeweb за 999 рублей. Готовые файлы поместил в папку /etc/ssl/mail

Команда для генерации

```
openssl req -new -x509 -days 1461 -nodes -out /etc/ssl/mail/cert.pem -keyout
/etc/ssl/mail/cert.key -subj "/C=RU/ST=SPb/L=SPb/O=Global
Security/OU=IT/CN=mail.fellk.ru"
```

Включаем автозапуск postfix и делаем перезагрузку сервиса

```
systemctl enable postfix
```

```
systemctl restart postfix
```

Настройка Dovecot

Устанавливаем Dovecot с зависимостями для баз данных

```
apt install dovecot-imapd dovecot-pop3d dovecot-mysql
```

Меняем способ хранения сообщений

```
nano /etc/dovecot/conf.d/10-mail.conf
```

```
mail_location = maildir:/mail/%d/%u/
```

конфигурируем слушателя для аутентификации

```
nano /etc/dovecot/conf.d/10-master.conf
```

```
service auth {
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfixmail
    group = postfixmail
  }
  unix_listener auth-userdb {
    mode = 0600
    user = mail
    group = mail
  }
}

service stats {
    unix_listener stats-reader {
        user = mail
        group = mail
        mode = 0660
    }
    unix_listener stats-writer {
        user = mail
        group = mail
        mode = 0660
    }
}
```

Настройка аутентификации в Dovecot

```
nano /etc/dovecot/conf.d/10-auth.conf
```

```
#!include auth-system.conf.ext
```

```
!include auth-sql.conf.ext
```

Настройка шифрования

```
nano /etc/dovecot/conf.d/10-ssl.conf
```

```
ssl = required
```

```
ssl_cert = </etc/ssl/mail/cert.pem
```

```
ssl_key = </etc/ssl/mail/cert.key
```

Настройка создания каталогов подключения к почте

```
nano /etc/dovecot/conf.d/15-lda.conf
```

```
lda_mailbox_autocreate = yes
```

Подключение к базе данных

```
nano /etc/dovecot/conf.d/auth-sql.conf.ext
```

```
passdb {
  args = /etc/dovecot/dovecot-sql.conf.ext
}

userdb {
  args = /etc/dovecot/dovecot-sql.conf.ext
}
```

Редактируем файл работы с базой данных

```
nano /etc/dovecot/dovecot-sql.conf.ext
```

```
driver = mysql
connect = host=localhost dbname=postfixmail user=postfixmail
password=password123456
default_pass_scheme = MD5-CRYPT
password_query = SELECT password FROM mailbox WHERE username = '%u'
user_query = SELECT maildir, 1024 AS uid, 1024 AS gid FROM mailbox WHERE
username = '%u'
user_query = SELECT CONCAT('/mail/',LCASE(`domain`),'/',LCASE(`maildir`)),
1024 AS uid, 1024 AS gid FROM mailbox WHERE username = '%u'
```

Настройка слушателя dovecot

```
nano /etc/dovecot/dovecot.conf
```

```
listen = *
```

Включаем автозапуск dovecot и делаем перезагрузку

```
systemctl enable dovecot
```

```
systemctl restart dovecot
```

Проверка почты

В браузере заходим в админку http://10.0.1.18/postfixadmin/public/login.php

Переходим в Список доменов и создаем новый домен.

Далее переходим в Обзор и создаем тестовый ящик.

> Для проверки можно использовать, MS Outlook, Mozilla Thunderbird и другие подобные программы.
>
> Сервер: имя сервера или его IP-адрес (если указывать IP, то сертификат не будет работать).
>
> IMAP: 143 без шифрования или 993 с шифрованием
>
> POP3: 110 без шифрования или 995 с шифрованием
>
> SMTP: 25 без шифрования или 465 с шифрованием

Устанавливаем и настраиваем веб клиент Roundcube

> Вы можете установить себе другой веб клиент например, rainloop, AfterLogic WebMail Lite и другие. В моем случае рассмотрим именно roundcube.

Скачиваем программу

```
wget
https://github.com/roundcube/roundcubemail/releases/download/1.6.1/roundcube
mail-1.6.1-complete.tar.gz
```

Создаем папку для размещения пограммы

```
mkdir /var/www/html/webmail
```

Делаем распаковку в эту папку

```
tar -C /var/www/html/webmail -xvf roundcubemail-*.tar.gz --strip-components
1
```

Копируем шаблон конфига и редактируем его

```
cp /var/www/html/webmail/config/config.inc.php.sample
/var/www/html/webmail/config/config.inc.php
```

```
nano /var/www/html/webmail/config/config.inc.php
```

```
$config['db_dsnw'] = 'mysql://root:Ваш пароль@localhost/roundcubemail';

$config['enable_installer'] = true;

$config['smtp_pass'] = '';
```

Прописываем папки в этом же конфиге

```
$config['drafts_mbox'] = 'Drafts';

$config['junk_mbox'] = 'Junk';

$config['sent_mbox'] = 'Sent';

$config['trash_mbox'] = 'Trash';
```

```
$config['create_default_folders'] = true;
```

Задаем владельца apache на папку портала

```
chown -R www-data:www-data /var/www/html/webmail
```

Создаем базу roundcubemail

```
mysql -uroot -p
```

```
CREATE DATABASE roundcubemail DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci;
```

```
GRANT ALL PRIVILEGES ON roundcubemail.* TO root@localhost IDENTIFIED BY 'Ваш пароль';
```

```
quit;
```

Прогружаем данные

```
mysql -uroot -p roundcubemail < /var/www/html/webmail/SQL/mysql.initial.sql
```

Ставим допы для Roundcube

```
apt install php-pear php-intl php-ldap php-net-smtp php-gd php-imagick php-zip php-curl
```

```
apt install php-dev libmcrypt-dev
```

```
pecl channel-update pecl.php.net
```

```
pecl install mcrypt-1.0.4
```

Создать файл настройки

```
nano /etc/php/8.1/fpm/conf.d/99-mcrypt.ini
```

```
extension=mcrypt.so
```

В конфиге php

```
nano /etc/php/8.1/fpm/php.ini
```

```
date.timezone = "Europe/Moscow"

post_max_size = 70M

upload_max_filesize = 70M
```

> В моем случае разрешение на файлы 70 мегабайт, вы можете изменить как вам нужно

Перезагружаем php-fpm

```
systemctl restart php8.1-fpm
```

Настроим apache2

```
nano /etc/php/8.1/apache2/php.ini
```

```
upload_max_filesize = 70M

post_max_size = 70M
```

Перезагружаем apache2

```
systemctl restart apache2
```

> В моем случае разрешение на файлы 70 мегабайт, вы можете изменить как вам нужно

Открываем браузер и переходим по адресу http://10.0.1.18/webmail/installer/. В самом низу нажимаем по кнопке Next.

> Если кнопка будет неактивна, проверяем, что нет ошибок (NOT OK)

На следующей странице проверяем, что все пункты находятся в состоянии OK. Установка выполнена.

Редактируем конфиг roundcube

```
nano /var/www/html/webmail/config/config.inc.php
```

```
$config['enable_installer'] = false;
```

Удаляем папку с установочными скриптами

```
rm -rf /var/www/html/webmail/installer
```

И заходим в браузере по адресу http://10.0.1.18/webmail/.

Вводим в качестве логина адрес почты созданного пользователя и его пароль.

Если все прошло успешно, то вы молодец, но впереди еще работа по защите.

Установка и настройка Clamav + Amavisd

Ставим все необходимое

```
apt install amavisd-new clamav clamav-daemon spamassassin
```

Добавляем пользователя clamav в группу amavis

```
usermod -a -G amavis clamav
```

Редактируем конфиг amavis

```
nano /etc/amavis/conf.d/15-content_filter_mode
```

убираем комменты:

```
@bypass_virus_checks_maps = (
      \%bypass_virus_checks,  \@bypass_virus_checks_acl,
\$bypass_virus_checks_re);

@bypass_spam_checks_maps = (
       \%bypass_spam_checks,  \@bypass_spam_checks_acl,
\$bypass_spam_checks_re);
```

Далее редактируем

```
nano /etc/amavis/conf.d/50-user
```

Нужно добавить

```
$allowed_header_tests{'multiple'} = 0;
```

```
$allowed_header_tests{'missing'} = 0;
```

Включаем автозапуск и перезагружаем

```
systemctl enable clamav-daemon clamav-freshclam amavis
```

```
systemctl restart amavis clamav-daemon clamav-freshclam
```

Делаем изменения в postfix

```
nano /etc/postfix/main.cf
```

```
content_filter = scan:[127.0.0.1]:10024
```

Так же тут master.cf

```
nano /etc/postfix/master.cf
```

```
scan   unix  -  -  n  -  16  smtp
  -o smtp_send_xforward_command=yes
  -o smtp_enforce_tls=no

127.0.0.1:10025   inet  n  -  n  -  16  smtpd
  -o content_filter=
  -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
  -o smtpd_helo_restrictions=
  -o smtpd_client_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks_style=host
  -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Перезапуск postfix

```
systemctl restart postfix
```

Включаем автообновление антиспама

```
sa-update --nogpg --verbose
```

```
crontab -e
```

```
00 0 * * * /usr/bin/sa-update
```

```
00 0 - Время 0 часов 00 минут, вы выставляете нужное вам
```

Тестируем антиспам

Содержание в сообщении ниже

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Нужно отправить на вашу тестовую почту Лучше это делать через telnet

Письмо не доставится, в логе (/var/log/maillog) будет нечто следующее

```
... amavis[17688]: (17688-04) Blocked INFECTED (Eicar-Signature)
{DiscardedOutbound,Quarantined}, MYNETS LOCAL ...
... relay=127.0.0.1[127.0.0.1]:10024, delay=0.25, delays=0.19/0/0/0.06,
dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=17688-04 - INFECTED:
Eicar-Signature)
```

Второй тест контентный

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

В логах будет

```
... amavis[17689]: (17689-04) Blocked SPAM {DiscardedOutbound,Quarantined},
MYNETS LOCAL ...
... status=sent (250 2.7.0 Ok, discarded, id=17689-04 - spam)
```

Отдельные ящики для спама и вирусов

В конфиге

```
nano /etc/amavis/conf.d/50-user
```

прописываем:

```
$spam_quarantine_to = "spam\@fellk.ru";

$virus_quarantine_to = "virus\@fellk.ru";
```

Перезапуск amavis

```
systemctl restart amavis
```

> Пробуем еще раз тестовые отправки. Но предварительно у вас должны быть созданы эти почтовые ящики.

Антиспам Postfix

В конфиге main.cf

```
nano /etc/postfix/main.cf
```

Комментируем строку

```
# smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated
defer_unauth_destination
```

Вписываем

```
smtpd_client_restrictions =
#Разрешить доступ из доверенных сетей
        permit_mynetworks
#Разрешить доступ клиентам, прошедшим процедуру аутентификации  SMTP
        permit_sasl_authenticated
#Запретить некорректное использование команд конвейерной обработки
        reject_unauth_pipelining
#Разрешить доступ
        permit

smtpd_helo_restrictions =
#Разрешить доступ
        permit

smtpd_sender_restrictions =
#Разрешить доступ из доверенных сетей
        permit_mynetworks
```

```
#Разрешить доступ клиентам, прошедшим процедуру аутентификации SMTP
        permit_sasl_authenticated
        reject_non_fqdn_sender
        reject_unknown_sender_domain
#Разрешить доступ
        permit

smtpd_relay_restrictions =
#Разрешить доступ из доверенных сетей
        permit_mynetworks
#Разрешить доступ клиентам, прошедшим процедуру аутентификации SMTP
        permit_sasl_authenticated
        defer_unauth_destination

smtpd_recipient_restrictions =
#Разрешить доступ из доверенных сетей
        permit_mynetworks
#Разрешить доступ клиентам, прошедшим процедуру аутентификации SMTP
        permit_sasl_authenticated
#Запретить доступ, если адрес получателя сообщения имеет некорректный формат
        reject_non_fqdn_recipient
#Запретить Postfix быть открытым релеем
        reject_unauth_destination
#Запретить доступ, если для имени домена адреса получателя не существует A или MX
запись в DNS
        reject_unknown_recipient_domain
#Запретить доступ, если адрес получателя не может быть проверен
        reject_unverified_recipient
#Запретить доступ клиентам, не зарегистрированным в DNS
        reject_unknown_client_hostname
#Запретить доступ, если имя хоста, содержащееся в выданном клиентом приветствии, имеет
некорректный синтаксис
 reject_invalid_helo_hostname
#Запретить доступ, если имя хоста, содержащееся в выданном клиентом приветствии, не
является FQDN
        reject_non_fqdn_helo_hostname
#Запретить доступ, если для имени хоста, содержащемся в выданном клиентом приветствии,
не существует A или MX запись в DNS
        reject_unknown_helo_hostname
######Проверить адрес сети клиента по блэклистам######
        reject_rbl_client zombie.dnsbl.sorbs.net,
        reject_rbl_client work.rsbs.express.ru,
        reject_rhsbl_sender dsn.rfc-ignorant.org
##Вызывает проблемы с отправкой и доставкой почты##        reject_rbl_client
bl.spamcop.net
##Вызывает проблемы с отправкой и доставкой почты##        reject_rbl_client
cbl.abuseat.org
##Вызывает проблемы с отправкой и доставкой почты##        reject_rbl_client
dul.ru
##Вызывает проблемы с отправкой и доставкой почты##        reject_rbl_client
dnsbl.abuse.ch
```

```
##Вызывает проблемы с отправкой и доставкой почты##      reject_rbl_client
zen.spamhaus.org,
##Вызывает проблемы с отправкой и доставкой почты##      reject_rbl_client
multihop.dsbl.org,
##Вызывает проблемы с отправкой и доставкой почты##      reject_rbl_client
dnsbl.sorbs.net,

#Проверить, разрешен ли адрес отправителя сообщения в файле, являющемся параметром
данного ограничения
        check_sender_access hash:/etc/postfix/sender_access
#Разрешить доступ
        permit
```

Перезагрузка Postfix

```
systemctl restart postfix
```

Обучение антиспама

```
sa-learn --spam /mail/fellk.ru/*/{.\&BCEEPwQwBDw-,.Spam,.Junk\ E-
mail,.Junk}/cur
```

> Данная команда ищет спам в папках у пользователей и таким образом происходит обучение.

Убрать некорректные срабатывания можно так

```
sa-learn --ham /mail/fellk.ru/spam\@fellk.ru/.Ham/cur
```

Статистика по обучению спама

```
sa-learn --dump magic
```

Выводим почту во внешку

rDNS

Для создания записи пишите или звоните в поддержку вашего провайдера и просите его сделать данную запись, предоставив ему информацию из команды

```
postconf -n myhostname
```

или

```
hostname
```

A-запись

Настраивается на вашем хостинге. Выглядит так

SPF запись

Настраивается на вашем хостинге. Выглядит так

DMARC запись

Настраивается на вашем хостинге. Выглядит так

DKIM запись

Создать папку для ключей

```
mkdir -p /var/lib/dkim
```

Генерируем последовательность

```
amavisd-new genrsa /var/lib/dkim/fellk.ru.pem 1024
```

Ставим нужные права

```
chown amavis:amavis /var/lib/dkim/*.pem
```

```
chmod 0400 /var/lib/dkim/*.pem
```

В конфиге amavisd редактируем

```
nano /etc/amavis/conf.d/20-debian_defaults
```

```
#$inet_socket_port = 10024;
$inet_socket_port = [10024,10026];

$forward_method = 'smtp:[127.0.0.1]:10025';
$notify_method = $forward_method;
$interface_policy{'10026'} = 'ORIGINATING';
$policy_bank{'ORIGINATING'} = {
    originating => 1,
    smtpd_discard_ehlo_keywords => ['8BITMIME'],
    os_fingerprint_method => undef,
    bypass_banned_checks_maps => [1],
    bypass_header_checks_maps => [1],
    bypass_banned_checks_maps => [1],
    virus_admin_maps => ["virusalert\@$mydomain"],
};
```

В файле 50-user добавляем

```
nano /etc/amavis/conf.d/50-user
```

```
$enable_dkim_verification = 1;
$enable_dkim_signing = 1;
dkim_key('fellk.ru', "dkim", "/var/lib/dkim/fellk.ru.pem");
@dkim_signature_options_bysender_maps = ( {
   "test.ru" => { d => "fellk.ru", a => 'rsa-sha256', ttl => 10*24*3600 },
});
```

Перезапускаем amavis

```
systemctl restart amavis
```

Проверить DKIM последовательность для домена можно так

```
amavisd-new showkeys
```

будет что-то вроде этого

```
; key#1 1024 bits, i=dkim, d=fellk.ru, /var/lib/dkim/fellk.ru.pem
dkim._domainkey.fellk.ru.        3600 TXT (
  "v=DKIM1; p="
  "VIDfMA0kh1jVbGBwY2Nx3IgEMgCNRDCRiQKBgQC23iOK+39mY9972KNNGKETJo8n/Heg"
  "x6eMYXsp1unAdo2EBJDFU35CNRDCRiQKBgQC23iOK+39mYBxsnIl1Jo8n/Heg"
  "x6eMA0kh1jVbGBZrREVZYTEAQUAA4CNRh1jNWGQIF38KWYTE+uPOwtAbXEeRLG/Vz5"
  "zyQuIRDCKSHWUGN2461SFG3iOQAB")
```

Теперь нужно на хостинге прописать эти данные. Выглядит так

Проверяем настройки DKIM

```
amavisd-new testkeys
```

Донастраиваем postfix

```
nano /etc/postfix/master.cf
```

```
smtp      inet  n       -       y       -       -       smtpd
  -o content_filter=scan:[127.0.0.1]:10026

submission   inet  n  -  n  -  -  smtpd
  -o content_filter=scan:[127.0.0.1]:10026

smtps   inet  n  -  n  -  -  smtpd
  -o content_filter=scan:[127.0.0.1]:10026

127.0.0.1:10027   inet  n  -  n  -  16  smtpd
  -o content_filter=
  -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
  -o smtpd_helo_restrictions=
  -o smtpd_client_restrictions=
  -o smtpd_sender_restrictions=
```

```
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks_style=host
  -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Перезапускаем postfix

```
systemctl restart postfix
```

Настраиваем Roundcube

```
nano /var/www/html/webmail/config/config.inc.php
```

Строки

```
$config['smtp_server'] = '';
$config['smtp_port'] = 25;
```

заменить на

```
$config['smtp_server'] = 'tls://localhost';
$config['smtp_port'] = 587;
```

> Проверить сервер можно тут:
>
> https://spamtest.smtp.bz

Настройка квот почты

В файле10-mail.conf

```
nano /etc/dovecot/conf.d/10-mail.conf
```

снимаем коммент или прописываем строку

```
mail_plugins = $mail_plugins quota
```

В файле 20-imap.conf

```
nano /etc/dovecot/conf.d/20-imap.conf
```

Снимаем комментарий или прописываем строку

```
protocol imap {
  mail_plugins = $mail_plugins imap_quota
}
```

В файле 10-master.conf

```
nano /etc/dovecot/conf.d/10-master.conf
```

редактируем строки как показано ниже

```
service dict {
    unix_listener dict {
    mode = 0660
    user = mail
    group = mail
  }
}
```

user и group - это все те же что создавались ранее вами

В файле 90-quota.conf

```
nano /etc/dovecot/conf.d/90-quota.conf
```

Добавляем строки или убираем коммент с них

```
plugin {
  quota = dict:User quota::proxy::quota
}
```

В файле dovecot.conf

```
nano /etc/dovecot/dovecot.conf
```

Убираем коммент или добавляем строки

```
dict {
  quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
}
```

В файле dovecot-dict-sql.conf.ext

```
nano /etc/dovecot/dovecot-dict-sql.conf.ext
```

Прописываем настройки

```
connect = host=localhost dbname=fellk user=root password=Ваш пароль
map {
  pattern = priv/quota/storage
  table = quota2
  username_field = username
  value_field = bytes
}
map {
  pattern = priv/quota/messages
  table = quota2
  username_field = username
  value_field = messages
}
```

Редактируем или дописываем в файле dovecot-sql.conf.ext

```
nano /etc/dovecot/dovecot-sql.conf.ext
```

```
user_query = SELECT CONCAT('/mail/',LCASE(`domain`),'/',LCASE(`maildir`)),
1024 AS uid, 1024 AS gid, CONCAT('*:bytes=', quota) AS quota_rule FROM
mailbox WHERE username = '%u'
```

Проверяем конфигурационный файл dovecot

```
doveconf
```

если нет ошибок, делаем рестарт

```
systemctl restart dovecot
```

Проверка работы квот

Для проверки используем команду

```
doveadm quota get -u test@fellk.ru
```

Прописывать квоты нужно в веб интерфейсе в каждый почтовый ящик

Информирование при превышении квот

В файле 90-quota.conf

```
nano /etc/dovecot/conf.d/90-quota.conf
```

Редактируем строки

```
plugin {
  quota_warning = storage=95%% quota-warning 95 %u
  quota_warning2 = storage=80%% quota-warning 80 %u
}
```

Можете указать свои значения превышения

В разделе service quota-warning редактируем все как ниже

```
service quota-warning {
  executable = script /usr/local/bin/quota-warning.sh
  user = dovecot
  unix_listener quota-warning {
    user = mail
  }
}
```

Скрипт оповещения quota-warning.sh

```
nano /usr/local/bin/quota-warning.sh
```

```
cat << EOF | /usr/libexec/dovecot/dovecot-lda -d $2 -o
"plugin/quota=maildir:User quota:noenforcing"
Content-Type: text/html; charset=utf-8
From: Администратор почты <admin@fellk.ru>
Subject: Предупреждение о превышении квоты на почтовый ящик
X-Priority: 2

<p>Размер Вашего почтового ящика $1% от установленного ограничения.<br>
Удалите большие письма с вложениями, сделайте архивацию или обратитесь за помощью в
ИТ отдел.</p>
EOF
```

Прописываем права на файл

```
chmod +x /usr/local/bin/quota-warning.sh
```

Тестируем скрипт

```
/usr/local/bin/quota-warning.sh 80 test@fellk.ru
```

Рестарт dovecot

```
systemctl restart dovecot
```

Для Outlook переводим папки на русский

Редактируем файл 15-mailboxes.conf

```
nano /etc/dovecot/conf.d/15-mailboxes.conf
```

В блоке namespace inbox редактируем

```
namespace inbox {
```

```
  mailbox Черновики {
    auto = subscribe
    special_use = \Drafts
  }
  mailbox Drafts {
    auto = no
    special_use = \Drafts
  }
  mailbox Спам {
    auto = subscribe
    special_use = \Junk
  }
  mailbox Junk {
    auto = no
    special_use = \Junk
  }
  mailbox Spam {
    auto = no
    special_use = \Junk
  }
  mailbox "Junk E-mail" {
    auto = no
    special_use = \Junk
  }
  mailbox Удаленные {
    auto = subscribe
    special_use = \Trash
  }
  mailbox Trash {
    auto = no
    special_use = \Trash
  }
  mailbox "Deleted Messages" {
    auto = no
    special_use = \Trash
  }
  mailbox Отправленные {
    auto = subscribe
    special_use = \Sent
  }
  mailbox Sent {
    auto = no
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    auto = no
    special_use = \Sent
  }
  mailbox "Sent Items" {
    auto = no
    special_use = \Sent
```

```
  }
}
```

Имейте ввиду что если вы пользуетесь с одного почтового ящика и Outlook и web интерфейсом, то у вас будет отображаться в Outlook и русские папки и английские, в английские будут валиться письма с web интерфейса, а в русские будут из Outlook.

Для применения настроек перезапускаем dovecot

```
systemctl restart dovecot
```

Настройка ограничения вложений

Начнем с файла

```
nano /etc/postfix/main.cf
```

Размер почтового ящика Для установки квоты на почтовые ящики редактируем следующее

```
mailbox_size_limit = 734003200
virtual_mailbox_limit = 734003200
message_size_limit = 73400320
```

Я ставлю 70 МБ - в файле это выглядит все в байтах как 734003200

Если не нужны ограничения, ставим 0:

После редактирования применяем изменения

```
systemctl reload postfix
```

Далее в файле:

```
nano /etc/php/7.4/apache2/php.ini
```

Находим и редактируем

```
post_max_size = 70M

upload_max_filesize = 70M
```

И не забываем о перезапуске

```
systemctl restart apache2
```

Возможные ошибки и их решения

решается данная проблема одной-двумя командами, в зависимости что указано в выводе ошибки

```
a2enmod rewrite
```

```
a2enmod ssl
```

Если не отправляются вложения из веб интерфейса Roundcube

Нужно отредактировать конфиг

```
nano /var/www/html/webmail/config/config.inc.php
```

добавив в него строку

```
$config['temp_dir'] = '/tmp/';
```