Postfix + Dovecot + Postfixadmin + Roundcube + Postgrey + DKIM

Настройка системы:

```
# cat /etc/hosts
127.0.0.1 localhost localhost.tst-amo.net.ua localhost4 localhost4.tst-amo.net.ua
::1 localhost localhost.tst-amo.net.ua localhost6 localhost6.tst-amo.net.ua

192.168.1.41 mail mail.tst-amo.net.ua
192.168.1.41 mail.tst-amo.net.ua.
```

```
# cat /etc/aliases

# Basic system aliases -- these MUST be present.
mailer-daemon: postmaster
postmaster: root
root: pm@tst-amo.net.ua # учетка на которую будет пересылаться почта root

# General redirections for pseudo accounts.
bin: root
daemon: root
```

```
# hostname
tst.tst-amo.net.ua
```

Очень желателен PTR (прописывается у провайдера по заявке, у моего нельзя)

Например:

```
# nslookup 222.444.22.63
Server: 192.168.1.41
Address: 192.168.1.41#53

Non-authoritative answer:
```

222.444.22.63.in-addr.arpa name = mail.domen.ua.

Предполагается, что уже установлены и настроены MySQL, nginx.

1. MySQL

Создаем базу данных:

```
# mysql -uroot -p
MariaDB [(none)]> CREATE DATABASE postfix;
Query OK, 1 row affected (0.03 sec)
MariaDB [(none)]> GRANT ALL PRIVILEGES ON postfix.* TO 'postfix'@'localhost' IDENTIFIED BY 'mypassword';
Query OK, 0 rows affected (0.10 sec)
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.01 sec)
MariaDB [(none)]> quit
```

2. Postfixadmin

```
# wget -q -O - "https://downloads.sourceforge.net/project/postfixadmin/postfixadmin/postfixadmin-3.2/postfixadmin-3.2.tar.gz" | tar -xzf - -C /home/www/
# yum install php56w-imap
# chown -R nginx:www-data /home/www/postfixadmin
```

– где nginx:www-data – пользователь под которым запускается nginx и группа

После обновления сменился владелец /var/lib/php/session и выдало ошибку в браузере

Invalid token

в логах ругань на permission, так как, владельцем стал root:apache:

2018/08/18 08:55:06 [error] 1786#0: *9149 FastCGI sent in stderr: "PHP message: PHP Warning: session_start(): open(/var/lib/php/session/sess_7p6c8kjkosj36d0lehjjr4eeg
6, O_RDWR) failed: Permission denied (13) in

```
/home/www/postfixadmin/common.php on line 26
PHP message: PHP Warning: session_start(): open(/var/lib/php/session/sess_7p6c8kjkosj36d0lehjjr4eeg6, O_RDWR) failed: Permission denied (13) in /home/www/postfixadmin
/public/login.php on line 84" while reading response header from upstream, client: 192.168.1.1, server: tst-amo.net.ua, request: "GET /postfixadmin/public/login.php HT
TP/2.0", upstream: "fastcgi://unix:/var/run/php-fpm/php-fpm.sock:", host: "tst-amo.net.ua"
2018/08/18 08:55:06 [error] 1786#0: *9149 FastCGI sent in stderr: "PHP message: PHP Warning: Unknown: open(/var/lib/php/session/sess_7p6c8kjkosj36d0lehjjr4eeg6, O_RDW
R) failed: Permission denied (13) in Unknown on line 0
```

Лечим:

```
# chown -R nginx:www-data /var/lib/php/session
```

У меня выдавало ошибку на отсутствие директории *templates_c*:

```
# mkdir postfixadmin/templates_c
# chown nginx:www-data templates_c
```

Заходить в сетап:

https://tst-amo.net.ua/postfixadmin/public/setup.php

добавить

```
$CONF['setup_password'] = '422962da717c2abb5408efe.......b2fa22dd9f7d1bc01835c9e59a';
```

После настройки заходим и создаем домен, ящики и т.д.

https://tst-amo.net.ua/postfixadmin/public/login.php

3. Postfix – виртуальные пользователи

Создаем сначала групу vmail с идентификатором 1024:

```
# groupadd -g 1024 vmail
```

а потом добавляем туда пользователя:

```
# useradd -d /home/vmail -g 1024 -u 1024 vmail -m
```

Добавить в /etc/postfix/main.cf

```
 ........
 virtual_mailbox_base = /home/vmail
 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

# Транспорт
virtual_transport = dovecot
dovecot_destination_recipient_limit = 1

…..

smtpd_recipient_restrictions =
    check_client_access hash:/etc/postfix/blacklist-IP
    permit_mynetworks
    permit_sasl_authenticated
    check_recipient_access hash:/etc/postfix/recipient-list
    reject_non_fqdn_recipient
    reject_unauth_destination
    reject_unknown_recipient_domain
    reject_unverified_recipient
    permit
```

Здесь правило reject_unauth_destination – должно запрещать открытый релей через ваш сервер

Содержимое служебных файлов:

```
[root@tst postfix]# cat mysql_virtual_alias_maps.cf
user = postfix
password = mypassword
```

```
hosts = localhost
dbname = postfix
query = SELECT goto FROM alias WHERE address='%s' AND active =
'1'

[root@tst postfix]# cat mysql_virtual_domains_maps.cf
user = postfix
password = mypassword
hosts = localhost
dbname = postfix
query = SELECT domain FROM domain WHERE domain='%u'

[root@tst postfix]# cat mysql_virtual_mailbox_maps.cf
user = postfix
password = mypassword
hosts = localhost
dbname = postfix
query = SELECT CONCAT(domain,'/',maildir) FROM mailbox WHERE
username='%s' AND active = '1'

[root@tst postfix]# cat access_sender
tst-amo.net.ua OnlyFromMyUsers

[root@tst postfix]# cat blacklist
#spam@net.ua REJECT
#info@uni.ka REJECT Your e-mail was banned!
#acc@tst1.pp.ua REJECT Your e-mail was banned!
#s@i.ua REJECT SPAM!!!
/.*@tst-amo\.net\.ua/i REJECT You are not imp.kiev.ua, this is
my name!!!

advocatov.com REJECT SPAM!!!
bilabonges.eu REJECT SPAM!!!
cloudlite.eu REJECT SPAM!!!
deals@save.spirit-airlines.com REJECT SPAM!!!
domrike.eu REJECT SPAM!!!
saffiano-double.ru REJECT SPAM!!!
whilsacom.eu REJECT SPAM!!!

[root@tst postfix]# cat blacklist-IP
1.52.38.29 REJECT Your IP is spam
2.90.145.125 REJECT Your IP is spam
5.235.7.171 REJECT Your IP is spam
```

```
37.104.210.18 REJECT Your IP is spam
37.106.204.58 REJECT Your IP is spam
42.113.159.236 REJECT Your IP is spam
42.116.220.21 REJECT Your IP is spam
43.250.80.131 REJECT Your IP is spam
45.244.118.151 REJECT Your IP is spam
```

```
[root@tst postfix]# cat header_checks
# Для спама
/^X-Spam-Level:.*\*{12,}.*/ REDIRECT spam@uni.ka
# Для вложений
/^(.*)name=\"(.*)\.(exe|bat|cmd|mp3)\"$/  REJECT  Attachment
type not allowed. File "$2" has unacceptable extension: "$3"
```

```
[root@tst postfix]# cat hello_access
mail.tst-amo.net.ua REJECT Don't use my server name!!!
```

```
[root@tst postfix]# cat recipient-list
# For these users to receive all
/^postmaster\@/ OK
/^hostmaster\@/ OK
/^abuse\@/ OK
/^webmaster\@/ OK
## Users
#/^mfint\@/ OK
#/^metall\@/ OK
```

```
[root@tst postfix]# cat whitelist
#-------------- Nuzhno_IMP ----------------
.nas.gov OK
@nas.gov OK
.domen.kiev.ua OK
@domen.kiev.ua OK

#-------------- Cheff other
@mpiyt-shalle.4mpg.de OK
.mpiyt-shalle.4mpg.de OK
```

4. Amavisd-new, ClamAV

This will install amavisd-new and a bunch of dependencies, and clamav + freshclam. It will also install SpamAssassin by default.

```
# yum install amavisd-new clamav clamav-update freshclam
```

Edit amavisd.conf.

```
# vim /etc/amavisd/amavisd.conf
```

Change the following lines like this…

```
$mydomain = ‘domain.com’; # a convenient default for other settings
$myhostname = 'mail.domain.com’; # must be a fully-qualified domain name and same as reverse DNS lookup
```

Make sure everything is set in postfix’s configuration file master.cf

```
# vim /etc/postfix/master.cf
```

On top of master.cf, you should have something like…

```
smtp inet n - n - - smtpd
  -o smtpd_sasl_auth_enable=yes
  -o receive_override_options=no_address_mappings
  -o content_filter=smtp-amavis:127.0.0.1:10024
```

…and on bottom, you should have something like…

```
#
 # spam/virus section
 #
 smtp-amavis unix - - n - 2 smtp
   -o smtp_data_done_timeout=1200
   -o disable_dns_lookups=yes
   -o smtp_send_xforward_command=yes
 127.0.0.1:10025 inet n - y - - smtpd
   -o content_filter=
   -o smtpd_helo_restrictions=
   -o smtpd_sender_restrictions=
   -o smtpd_recipient_restrictions=permit_mynetworks,reject
   -o mynetworks=127.0.0.0/8
   -o smtpd_error_sleep_time=0
```

```
   -o smtpd_soft_error_limit=1001
   -o smtpd_hard_error_limit=1000
   -o receive_override_options=no_header_body_checks
   -o smtpd_helo_required=no
   -o smtpd_client_restrictions=
   -o smtpd_restriction_classes=
   -o disable_vrfy_command=no
   -o strict_rfc821_envelopes=yes
```

Stop the postfix daemon.

```
# service postfix stop
```

Start Spamassassin, Amavisd-new and ClamAV daemons.

Проверка синтаксиса Spamassassin

```
# spamassassin --lint
```

Обновляем правила Spamassassin:

```
# sa-update --nogpg
```

Обновляем базы Spamassassin

```
# sa-update -v
```

```
# service spamassassin start
# service amavisd start
# service postfix start
```

5. Postgrey

```
# yum install postgrey
```

```
smtpd_recipient_restrictions =
   check_client_access hash:/etc/postfix/blacklist-IP
   permit_mynetworks
   permit_sasl_authenticated
   check_recipient_access hash:/etc/postfix/recipient-list
   reject_non_fqdn_recipient
   reject_unauth_destination
 ## POSTGREY
```

```
                                        #check_policy_service
unix:/var/spool/postfix/postgrey/socket
   check_policy_service inet:127.0.0.1:10023
 ##
   reject_unknown_recipient_domain
   reject_unverified_recipient
   permit
```

строчка “check_policy_service unix:/var/spool/postfix/postgrey/socket,” или “check_policy_service inet:127.0.0.1:10023” должна быть обязательно прописана после строчки параметра “reject_unauth_destination”, как на примере выше.

По ману запускать нужно так:

```
# man postgrey
# postgrey --inet=10023 -d

# systemctl start postgrey && systemctl enable postgrey
# systemctl reload postfix
```

6. OpenDKIM

```
# yum install -y opendkim
```

Генерируем ключ:

```
# opendkim-genkey -D /etc/opendkim/ --domain tst-amo.net.ua --selector relay
# cd /etc/opendkim
# chown :opendkim /etc/opendkim/*
# chmod g+r /etc/opendkim/*

# cp opendkim.conf opendkim.conf_orig
# cat opendkim.conf_orig | grep "^[^#]" > opendkim.conf
```

Правим opendkim.conf до состояния:

```
[root@tst etc]# cat opendkim.conf
AutoRestart Yes
AutoRestartRate 10/1h
Umask 002
```

```
Syslog yes
SyslogSuccess Yes
LogWhy Yes
Canonicalization relaxed/simple
ExternalIgnoreList refile:/etc/opendkim/TrustedHosts
InternalHosts refile:/etc/opendkim/TrustedHosts
KeyTable refile:/etc/opendkim/KeyTable
SigningTable refile:/etc/opendkim/SigningTable
Mode sv
PidFile /var/run/opendkim/opendkim.pid
SignatureAlgorithm rsa-sha256
UserID opendkim:opendkim
Socket inet:12301@localhost
```

Создаем служебные файлы:

```
# touch /etc/opendkim/TrustedHosts
# touch /etc/opendkim/KeyTable
# touch /etc/opendkim/SigningTable
```

Их содержимое:

```
# cat /etc/opendkim/KeyTable
 relay._domainkey.tst-amo.net.ua tst-amo.net.ua:relay:/etc/opendkim/relay.private
```

```
# cat /etc/opendkim/SigningTable
 *@tst-amo.net.ua relay._domainkey.tst-amo.net.ua
```

```
# cat /etc/opendkim/TrustedHosts
 127.0.0.1
 localhost
 *.tst-amo.net.ua
 #host.example.com
 #192.168.1.0/24
```

Запускаем сервис:

```
# systemctl start opendkim.service
# systemctl enable opendkim.service
# systemctl status opendkim.service
```

Добавляем в main.cf для Postfix

```
# nano /etc/postfix/main.cf
# DKIM
milter_protocol = 2
milter_default_action = accept
smtpd_milters = inet:127.0.0.1:12301
non_smtpd_milters = $smtpd_milters

# service postfix reload
```

для BIND

```
# nano /var/named/chroot/var/named/tst-amo.net.ua.zone
  relay._domainkey IN TXT ( "v=DKIM1; k=rsa; "
"p=MIGfMA0GCSqGSIb3DQEBAQUAA......k02pIg+TwIDAQAB" )
```

```
# service named-chroot reload
# service named-chroot status
```

Проверяем.

7 . Dovecot

```
# yum install dovecot dovecot-mysql dovecot-pigeonhole
```

Dovecot quota

```
# nano /etc/dovecot/conf.d/10-mail.conf
mail_plugins = $mail_plugins quota
```

```
# nano /etc/dovecot/conf.d/20-imap.conf
protocol imap {
   mail_plugins = $mail_plugins imap_quota
}
```

```
# nano /etc/dovecot/conf.d/10-master.conf
service dict {
    unix_listener dict {
       mode = 0660
       user = vmail
       group = vmail
    }
}
```

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

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

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

# nano /etc/dovecot/dovecot-dict-sql.conf.ext
connect  =  host=localhost  dbname=postfix  user=postfix
password=mypassword
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
}
map {
    pattern = shared/expire/$user/$mailbox
    table = expires
    value_field = expire_stamp
fields {
    username = $user
    mailbox = $mailbox
   }
}

# nano /etc/dovecot/dovecot-sql.conf.ext
# Database driver: mysql, pgsql, sqlite
 driver = mysql
  connect  =  host=localhost  dbname=postfix  user=postfix
password=mypassword
 default_pass_scheme = MD5-CRYPT

#
 password_query = SELECT `username` as `user`, `password` FROM
```

```
`mailbox` WHERE `username` = '%n@%d' AND `active`='1'

#
 user_query = SELECT CONCAT('/var/vmail/', `maildir`) AS \
 `home`, 1024 AS `uid`, 1024 AS `gid`, concat('dict:storage=', \
 CAST(ROUND(quota / 1024) AS CHAR), '::proxy::sqlquota') \
 AS quota, CONCAT('*:storage=', CAST(quota AS CHAR), 'B') AS quota_rule \
 FROM `mailbox` WHERE `username` = '%n@%d' AND `active`='1'

# Query to get a list of all usernames.
 iterate_query = SELECT username AS user FROM mailbox
```

```
# systemctl restart dovecot
```

Просмотр квоты пользователя(также можно просмотреть в WEB-интерфейсе PostfixAdmin).

```
# doveadm quota get -u username@example.com
```

Включение оповещений при превышении квоты

```
# nano /etc/dovecot/conf.d/90-quota.conf
plugin {
 # LDA/LMTP allows saving the last mail to bring user from under quota to
 # over quota, if the quota doesn't grow too high. Default is to allow as
 # long as quota will stay under 10% above the limit. Also allowed e.g. 10M.
   quota_rule = *:storage=500M
   quota_rule2 = Trash:storage=+100M
   quota_rule3 = Junk:ignore
   quota_grace = 10%%
}

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

##
## Quota backends
```

```
##

# Multiple backends are supported:
# dirsize: Find and sum all the files found from mail directory.
# Extremely SLOW with Maildir. It'll eat your CPU and disk I/O.
# dict: Keep quota stored in dictionary (eg. SQL)
# maildir: Maildir++ quota
# fs: Read-only support for filesystem quota

plugin {
   #quota = dirsize:User quota
   quota = maildir:User quota::proxy::quota

   #quota = dict:User quota::proxy::quota
   #quota = fs:User quota
}

# Multiple quota roots are also possible, for example this gives each user
# their own 100MB quota and one shared 1GB quota within the domain:
plugin {
   #quota = dict:user::proxy::quota
   #quota2 = dict:domain:%d:proxy::quota_domain
   #quota_rule = *:storage=102400
   #quota2_rule = *:storage=1048576
}
```

```
# nano /etc/dovecot/quota-warning.sh
#!/bin/sh
PERCENT=$1
USER=$2
cat << EOF | /usr/libexec/dovecot/dovecot-lda -d $USER -o "plugin/quota=maildir:User quota:noenforcing"
From: postmaster@tst-amo.net.ua
Subject: quota warning
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit
To: $USER
```

```
Внимание!
Ваш ящик заполнен на $PERCENT%.

Attention!
Your mailbox is now $PERCENT% full.
EOF
```