Установка Postfix,MySQL,SpamAssasson,ClamAV в FreeBSD

1. Установка MySQL

Cd /usr/ports/databases/mysql50-server

Make all install clean

Echo ‘mysql\_enable=”YES”’ >> /etc/rc.conf

/usr/local/etc/rc.d/mysql-server start

mysql –u root mysql

update user set password=PASSWORD(‘mysql\_root\_password’) where user=’root’;

flush privileges;

копируем файл настроек

cp /usr/local/share/mysql/my-medium.cnf /var/db/my.cnf

Меняем в нем параметры

Max\_allowed\_packet=10M

Innodb\_data\_home\_dir=/var/db/mysql

Innodb\_data\_file\_path = ibdata1:10M:autoextend

Innodb\_log\_group\_home\_dir = /var/db/mysql

Innodb\_buffer\_pool\_size = 16M

Innodb\_additional\_mem\_pool\_size = 2M

Innodb\_lock\_wait\_timeout = 50

Innodb\_log\_file\_size = 5M

Innodb\_log\_buffer\_size = 8M

Innodb\_flush\_log\_at\_trx\_commit = 1

Рестарт

/usr/local/etc/rc.d/mysql-server restart

1. Установка Dovecot (pop3/imap server)

Cd /usr/ports/mail/dovecot

Make all install clean (выбрать MYSQL)

Echo ‘dovecot\_enable=”YES”’ >> /etc/rc.conf

Конф файлы

Cp /usr/local/share/examples/dovecot/dovecot.conf /usr/local/etc/dovecot.conf

Cp /usr/local/share/examples/dovecot/dovecot-sql.conf /usr/local/etc/dovecot-sql.conf

Отредактировать конф файл

Protocols = imap pop3

Mail\_location = maildir:/usr/local/virtual/%d/%n

Редактируем файл dovecot-sql.conf

Driver = mysql

Connect = host=localhost dbname=postfix user=postfix password=postfix\_mysql\_password

Default\_pass\_scheme = MD5

Password\_query = select password from mailbox where username = ‘%u’

User\_query = select maildir, 125 AS uid, 125 AS gid, CONCAT(‘maildir:storage=’, FLOOR( quota / 1024 )

Если квоты не нужны то последнюю часть убрать

1. Установка Postfix

Cd /usr/ports/mail/postfix

Make all install clean

Выбрать параметры dovecot,tls,bdb,mysql,vda

/etc/rc.d/sendmail forcestop

убить все процессы sendmail

редактируем /etc/rc.conf

sendmail\_enable=”NO”

sendmail\_submit\_enable=”NO”

sendmail\_outbound\_enable=”NO”

sendmail\_msp\_queue\_enable=”NO”

postfix\_enable=”YES”

vi /etc/periodic.conf

daily\_clean\_hoststat\_enable=”NO”

daily\_status\_mail\_rejects\_enable=”NO”

daily\_status\_include\_submit\_mailq=”NO”

daily\_submit\_queuerun=”NO”

vi /usr/local/etc/postfix/main.cf

alias\_maps = hash:/etc/aliases

alias\_database = hash:/etc/aliases

#размер сообщения целиком

message\_size\_limit = 10240000

# SOFT BOUNCE

#

# The soft\_bounce parameter provides a limited safety net for

# testing. When soft\_bounce is enabled, mail will remain queued that

# would otherwise bounce. This parameter disables locally-generated

# bounces, and prevents the SMTP server from rejecting mail permanently

# (by changing 5xx replies into 4xx replies). However, soft\_bounce

# is no cure for address rewriting mistakes or mail routing mistakes.

#

soft\_bounce = no

# SASL CONFIG

#

broken\_sasl\_auth\_clients = yes

smtpd\_sender\_restrictions = permit\_sasl\_authenticated, permit\_mynetworks

smtpd\_recipient\_restrictions =

permit\_mynetworks,

permit\_sasl\_authenticated,

reject\_non\_fqdn\_sender,

reject\_non\_fqdn\_recipient,

reject\_unauth\_destination,

reject\_unauth\_pipelining,

reject\_invalid\_hostname,

smtpd\_sasl\_auth\_enable = yes

smtpd\_sasl\_authenticated\_header = yes

smtpd\_sasl\_local\_domain = $myhostname

smtpd\_sasl\_security\_options = noanonymous

smtpd\_sasl\_type = dovecot

smtpd\_sasl\_path = private/auth

# MySQL Configuration

#

virtual\_alias\_maps = proxy:mysql:/usr/local/etc/postfix/mysql\_virtual\_alias\_maps.cf

virtual\_gid\_maps = static:125

virtual\_mailbox\_base = /usr/local/virtual

virtual\_mailbox\_domains = proxy:mysql:/usr/local/etc/postfix/mysql\_virtual\_domains\_maps.cf

virtual\_mailbox\_limit = 51200000

virtual\_mailbox\_maps = proxy:mysql:/usr/local/etc/postfix/mysql\_virtual\_mailbox\_maps.cf

virtual\_minimum\_uid = 125

virtual\_transport = virtual

virtual\_uid\_maps = static:125

# Additional for quota support

# vda patch в портах FreeBSD по умолчанию накладывается

# Do we use Courier maildir++ quotas?

# Default: no

virtual\_maildir\_extended = yes

#virtual\_mailbox\_limit\_inbox = yes

virtual\_create\_maildirsize = yes

virtual\_mailbox\_extended = yes

virtual\_mailbox\_limit\_maps = proxy:mysql:/usr/local/etc/postfix/mysql\_virtual\_mailbox\_limit\_maps.cf

proxy\_read\_maps = $local\_recipient\_maps $mydestination $virtual\_alias\_maps

$virtual\_alias\_domains $virtual\_mailbox\_maps $virtual\_mailbox\_domains

$relay\_recipient\_maps $relay\_domains $canonical\_maps $sender\_canonical\_maps

$recipient\_canonical\_maps $relocated\_maps $transport\_maps $mynetworks

$virtual\_mailbox\_limit\_maps

virtual\_mailbox\_limit\_override = yes

virtual\_maildir\_limit\_message = Sorry, this user has overdrawn their diskspace quota. Please try again later.

virtual\_overquota\_bounce = yes

...

#myhostname = host.domain.tld

...

#mydomain = domain.tld

...

#mydestination = localhost.$mydomain, localhost

...

relay\_domains = proxy:mysql:/usr/local/etc/postfix/mysql\_relay\_domains\_maps.cf

отредактируем файл /usr/local/etc/postfix/mysql\_virtual\_alias\_maps.cf

user = postfix

password = postfix\_sql\_password

hosts = localhost

dbname = postfix

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

отредактируем файл /usr/local/etc/postfix/mysql\_virtual\_domains\_maps.cf

user = postfix

password = postfix\_sql\_password

hosts = localhost

dbname = postfix

query = SELECT domain FROM domain WHERE domain='%s' and backupmx = '0' and active = '1'

отредактируем файл /usr/local/etc/postfix/mysql\_virtual\_mailbox\_maps.cf

user = postfix

password = postfix\_sql\_password

hosts = localhost

dbname = postfix

query = SELECT maildir FROM mailbox WHERE username='%s' AND active = '1'

отредактируем файл /usr/local/etc/postfix/mysql\_virtual\_mailbox\_limit\_maps.cf

user = postfix

password = postfix\_sql\_password

hosts = localhost

dbname = postfix

query = SELECT quota FROM mailbox WHERE username='%s'

отредактируем файл /usr/local/etc/postfix/mysql\_relay\_domains\_maps.cf

user = postfix

password = postfix\_sql\_password

hosts = localhost

dbname = postfix

query = SELECT domain FROM domain WHERE domain='%s' and backupmx = '1'

Обеспечим безопастность файлов с паролями

chmod 640 /usr/local/etc/postfix/mysql\_\*

chgrp postfix /usr/local/etc/postfix/mysql\_\*

Редактируем aliases для доставки системных сообщений

/etc/aliases

root: [account@domain.com](mailto:account@domain.com)

/usr/bin/newaliases

Создадим директорию для наших виртуальных почтовых ящиков

mkdir /usr/local/virtual

chown -R postfix:postfix /usr/local/virtual

chmod -R 700 /usr/local/virtual

1. Установим Apache

cd /usr/ports/www/apache22

make all install clean

Отредактируем конфигурационный файл /usr/local/etc/apache22/httpd.conf:

ServerAdmin webmaster@domain.tld

ServerName www.domain.tld:80

# Various default settings

Include etc/apache22/extra/httpd-default.conf

# Secure (SSL/TLS) connections

Include etc/apache22/extra/httpd-ssl.conf

Отредактируем файл /usr/local/etc/apache22/extra/httpd-default.conf

ServerTokens Prod

...

ServerSignature Off

...

HostnameLookups Off

...

Отредактируем файл /usr/local/etc/apache22/extra/httpd-ssl.conf

...

ServerName www.domain.tld:443

...

ServerAdmin webmaster@domain.tld

...

Добавим Apache в автозапуск

echo 'apache22\_enable="YES"' >> /etc/rc.conf

/usr/local/etc/rc.d/apache22 start

1. PHP

cd /usr/ports/lang/php5

make all install clean

Не забудьте выбрать “APACHE” в меню установки.

Установим расширения для PHP.

cd /usr/ports/lang/php5-extensions

make all install clean

В меню установки необходимо выбрать “BCMATH“, “GETTEXT“, “IMAP“, “MCRYPT“, “MYSQL“, “MYSQLI“, “SESSION“, “SOCKETS“ и “WDDX”.

Скопируем файл /usr/local/etc/php.ini

cp /usr/local/etc/php.ini-production /usr/local/etc/php.ini

chmod 644 /usr/local/etc/php.ini

Отредактируем файл /usr/local/etc/php.ini

...

;;;;;;;;;;;;;;;;;;;;;;;;;

; Paths and Directories ;

;;;;;;;;;;;;;;;;;;;;;;;;;

; UNIX: "/path1:/path2"

include\_path = "."

Отредактируем файл конфигурации /usr/local/etc/apache22/httpd.conf

...

<IfModule dir\_module>

DirectoryIndex index.html index.php index.php5

</IfModule>

...

...

<IfModule mime\_module>

TypesConfig etc/apache22/mime.types

AddType application/x-compress .Z

AddType application/x-gzip .gz .tgz

AddType application/x-httpd-php .php

AddType application/x-httpd-php-source .phps

</IfModule>

Перезапустим Apache

apachectl restart

1. Postfixadmin

Установка Postfixadmin из портов

cd /usr/ports/mail/postfixadmin

make all install clean

Не забудьте в меню установки выбрать параметр “MYSQLI”.

Создадим базуPostfixAdmin

mysql -u root -p

(Enter MySQL root password)

>CREATE DATABASE postfix;

>CREATE USER 'postfix'@'localhost' IDENTIFIED BY 'postfix\_sql\_password';

>GRANT ALL PRIVILEGES ON `postfix` . \* TO 'postfix'@'localhost';

>FLUSH PRIVILEGES;

Защитим файлы PostfixAdmin

cd /usr/local/www/postfixadmin

find . -type f -exec chmod 640 {} \;

find . -type d -exec chmod 750 {} \;

Отредактируем файл /usr/local/www/postfixadmin/config.inc.php

$CONF['configured'] = true;

$CONF['postfix\_admin\_url'] = 'https://www.domain.tld/postfixadmin/';

$CONF['database\_type'] = 'mysqli';

$CONF['database\_host'] = 'localhost';

$CONF['database\_user'] = 'postfix';

$CONF['database\_password'] = 'postfix\_sql\_password';

$CONF['database\_name'] = 'postfix';

$CONF['database\_prefix'] = '';

$CONF['admin\_email'] = 'postmaster@domain.tld';

$CONF['default\_aliases'] = array (

'abuse' => 'abuse@domain.tld',

'hostmaster' => 'hostmaster@domain.tld',

'postmaster' => 'postmaster@domain.tld',

'webmaster' => 'webmaster@domain.tld'

);

$CONF['generate\_password'] = 'NO';

$CONF['page\_size'] = '20';

$CONF['domain\_path'] = 'YES';

$CONF['domain\_in\_mailbox'] = 'NO';

$CONF['aliases'] = '50';

$CONF['mailboxes'] = '50';

$CONF['maxquota'] = '1024';

$CONF['quota'] = 'YES';

$CONF['quota\_multiplier'] = '1048576';

$CONF['transport'] = 'NO';

$CONF['vacation'] = 'YES';

$CONF['vacation\_domain'] = 'autoreply.domain.tld';

$CONF['alias\_control\_admin'] = 'YES';

$CONF['special\_alias\_control'] = 'YES';

$CONF['show\_header\_text'] = 'YES';

$CONF['header\_text'] = ':: Postfix Admin ::';

$CONF['show\_footer\_text'] = 'YES';

$CONF['footer\_text'] = 'Return to domain.tld';

$CONF['user\_footer\_link'] = 'http://www.domain.tld/';

$CONF['welcome\_text'] = <<Hello,

Welcome to your new email account!

For questions or comments regarding your mail account,

please feel free to send an email to support@domain.tld.

Likewise, any other inqueries regarding ISP NAME or their

affiliates can be sent to the same address.

Also, don't forget to check your mail settings via Maia-

Mailguard located at https://www.domain.tld/maia-mailguard/.

Simply log into your account using your email address

and password. That's it! From Maia-Mailguard, you can

adjust your spam, virus, malware, whitelists, blacklists,

etc... This will put you in full control of your email so

you never miss anything important.

Thank you for using ISP NAME and enjoy your new email

account!

Regards,

ISP NAME Staff

support@domain.tld

EOM;

?>

$CONF['emailcheck\_resolve\_domain']='NO';

Создадим пользователя и группу Vacation

pw groupadd vacation

pw useradd vacation -c Virtual\ Vacation -d /nonexistent -g vacation -s /sbin/nologin

Создадим, наполним и обезопасим директорию vacation

cd /usr/ports/mail/p5-MIME-EncWords

make install clean

cd /usr/ports/mail/p5-Email-Valid

make install clean

cd /usr/ports/mail/p5-Mail-Sender

make install clean

cd /usr/ports/devel/p5-Log-Log4perl

make install clean

cd /usr/ports/devel/p5-Log-Dispatch

make install clean

mkdir /var/spool/vacation

cp /usr/local/www/postfixadmin/VIRTUAL\_VACATION/vacation.pl /var/spool/vacation/

chown -R vacation:vacation /var/spool/vacation/

chmod 700 /var/spool/vacation/

chmod 750 /var/spool/vacation/vacation.pl

touch /var/log/vacation.log /var/log/vacation-debug.log

chown vacation:vacation /var/log/vacation\*

Отредактируем скрипт /var/spool/vacation/vacation.pl

my $db\_type = 'mysql';

our $db\_host = 'localhost';

our $db\_user = 'postfix';

our $db\_pass = 'postfix\_sql\_password';

our $db\_name = 'postfix';

our $vacation\_domain = 'autoreply.domain.tld';

our $smtp\_server = 'localhost';

our $smtp\_server\_port =25;

our $logfile = "/var/log/vacation.log"; # specify a file name here for example: vacation.log

our $debugfile = "/var/log/vacation-debug.log"; # sepcify a file name here for example: vacation.debug

our $syslog = 1; # 1 if log entries should be sent to syslog

Добавим vacation фильтр в файл /usr/local/etc/postfix/master.cf:

Добавим в начало файла

vacation unix - n n - - pipe

flags=DRhu user=vacation argv=/var/spool/vacation/vacation.pl -f ${sender} ${recipient}

Добавим для vacation транспорт в файл /usr/local/etc/postfix/main.cf:

...

# TRANSPORT MAP

#

# See the discussion in the ADDRESS\_REWRITING\_README document.

transport\_maps = hash:/usr/local/etc/postfix/transport

vacation\_destination\_recipient\_limit = 1

...

Добавим в файл /usr/local/etc/postfix/transport

echo 'autoreply.domain.tld vacation:' >> /usr/local/etc/postfix/transport

Создадим для Postfix базу транспорт

postmap /usr/local/etc/postfix/transport

Создадим и отредактируем файл /usr/local/etc/apache22/Includes/postfixadmin.conf

Alias /postfixadmin/ "/usr/local/www/postfixadmin/"

<Directory "/usr/local/www/postfixadmin/">

Options Indexes

AllowOverride AuthConfig

Order allow,deny

Allow from all

</Directory>

Протестируем и перезапустим конфигурацию Apache.

apachectl configtest

apachectl graceful

Запустим необходимые приложения

/usr/local/etc/rc.d/mysql-server start

/usr/local/etc/rc.d/dovecot start

/usr/local/etc/rc.d/postfix start

Протестируем и назначим администратора PostfixAdmin.

Посетите страничку “http://domain.tld/postfixadmin/. Нажмине ссылку “setup” в тексте и посмотрите вывод, для того чтобы не возникло проблем. Сначала вам будет предложено ввести почтовый адрес и пароль для учетной записи ‘Administror’ в PostfixAdmin. Можно использовать любой адрес и пароль. После того как мы добавили учетную запись ‘Administrator’.

Удалите файл /usr/local/www/postfixadmin/setup.php (или переместите куда нибудь)

Добавим домен и пользователя в Postfix

Откроем страничку “http://domain.tld/postfixadmin/”

Введем имя пользователя и пароль для PostfixAdmin, указанный нами при установке. Выберем “Domain List”, “New Domain“ и заполним нужные поля. Дальше нажмите “Virtual List”, “Add Mailbox“ и заполните нужные поля.

1. SpamAssassin

Установим SpamAssassin из портов.

cd /usr/ports/mail/p5-Mail-SpamAssassin

make all install clean

В меню установки отключите “SPAMC” и обязательно выберете “GNUPG“, “MYSQL“, “RAZOR”.

Создадим пользователя “vscan”

pw groupadd vscan

pw useradd -n vscan -c Amavisd\ User -d /var/amavisd -g vscan -m

passwd vscan

Дважды введите пароль.

Создадим и отредактируем файл /usr/local/etc/mail/spamassassin/local.cf

use\_bayes 1

bayes\_store\_module Mail::SpamAssassin::BayesStore::MySQL

bayes\_sql\_dsn DBI:mysql:maia

bayes\_sql\_username vscan

bayes\_sql\_password vscan\_password

auto\_whitelist\_factory Mail::SpamAssassin::SQLBasedAddrList

user\_awl\_dsn DBI:mysql:maia

user\_awl\_sql\_username vscan

user\_awl\_sql\_password vscan\_password

bayes\_auto\_expire 0

# Change 192.168.1.\* to your actual internal/external address(es).

internal\_networks 192.168.1.0/24

trusted\_networks 192.168.1/24

Настроим отчеты RAZOR

su - vscan

razor-admin -discover

razor-admin -create

razor-admin -register -l -user=username@domain.tld -pass=some\_password

exit

Вышеупомянутый пользователь, должен быть пользователем, ящик которого вы проверяете. Это нужно системе razor2 для идентификации и отправки отчетов о спаме.

1. ClamAV

Установим Clam Anti-Virus из портов.

cd /usr/ports/security/clamav

make all install clean CLAMAVUSER=vscan CLAMAVGROUP=vscan

В меню достаточно оставить опции по умолчанию.

Добавим в файл /etc/make.conf параметры для установки.

Это поможет при обновлении программы из портов в дальнейшем избежать проблем.

echo 'CLAMAVUSER=vscan' >> /etc/make.conf

echo 'CLAMAVGROUP=vscan' >> /etc/make.conf

Добавим ClamAV в автозапуск системы.

echo 'clamav\_freshclam\_enable="YES"' >> /etc/rc.conf

echo 'clamav\_clamd\_enable="YES"' >> /etc/rc.conf

Запустим программы FreshClam и ClamAV:

/usr/local/etc/rc.d/clamav-clamd start

/usr/local/etc/rc.d/clamav-freshclam start

Дока по clamav+spamassassin, лучше не напишу ☺ http://www.opennet.ru/base/net/clamav\_setup.txt.html