Exim + Dovecot + MySQL

1. Устанавливаем Exim:

```
cd /usr/ports/mail/exim
make install clean
```

Опции (с заделом на будущее)

```
[x] CONTENT_SCAN Enable exiscan email content scanner
[x] DAEMON Install scripts to run as a daemon
[x] DISABLE_D_OPT Disable macros overrides using option -D
[x] DKIM Enable support for DKIM
[x] DNSSEC Enable DNSSEC validation
[x] DOCS Build and/or install documentation
[x] EMBEDDED_PERL Enable embedded Perl interpreter
[x] ICONV Enable header charset conversion
[x] LMTP RFC2033 SMTP over command pipe transport
[x] OCSP Enable OCSP stapling
[x] PRDR Enable Per-Recipient-Data-Response support
[x] SUID Install the exim binary suid root
——————————————————— SMTP Authorization
[x] AUTH_CRAM_MD5 Enable CRAM-MD5 authentication mechanisms
[x] AUTH_DOVECOT Enable Dovecot authentication mechanisms
[x] AUTH_PLAINTEXT Enable plaintext authentication
[x] AUTH_SPA Enable Secure Password Authentication
[x] SASLAUTHD Enable use of Cyrus SASL auth daemon
[x] PAM Enable PAM authentication mechanisms
[x] PASSWD Enable /etc/passwd lookups
——————————————————— Lookup support
[x] CDB Enable CDB-style lookups
[x] DNSDB Enable DNS-style lookups
[x] DSEARCH Enable directory-list lookups
[x] LSEARCH Enable wildcarded-file lookups
[x] MYSQL Enable mysql lookups
————————————————————— Supported storage formats
[x] MAILDIR Enable Maildir mailbox format
[x] MAILSTORE Enable Mailstore mailbox format
[x] MBX Enable MBX mailbox format
——————————————————— TLS support
(*) TLS TLS support
```

Редактируем conf файл

```
cd /usr/local/etc/exim
ee /configure
```

```
# CONF EXIM + MYSQL + DOVECOT + CLAMAV + POSTFIX + DSPAM
# Авторизация - довекот. квоты, кламав, БД в мускуле, dspam

# Имя нашей почтовой системы - HELO
primary_hostname = mail.tst-amo.pp.ua

# хост/БД/пользователь/пароль
mysql_servers = localhost/postfix/pOstFix/myPassWord

# Список доменов нашей почтовой системы
domainlist local_domains = ${lookup mysql{SELECT `domain` FROM
`domain`\
 WHERE `domain`='${domain}' AND `active`='1'}}

# Логгирование
log_selector = +all
#log_file_path = /var/log/exim/%D-%slog # Логирование будет
вида 20160924-mainlog and 20160924-rejetlog
log_file_path = /var/log/exim/%slog

# Список доменов, для которых наша почтовая система является
резервной
domainlist relay_to_domains = ${lookup mysql{SELECT `domain`
FROM `domain` \
 WHERE `domain`='${domain}' AND `active`='1'}}

hostlist relay_from_hosts = localhost : 127.0.0.1 :
192.168.1.0/24

acl_smtp_rcpt = acl_check_rcpt
acl_smtp_mime = acl_check_mime

# Прикручиваем антивирус - при условии, что exim собран
# с его поддержкой. В качестве антивиря юзаем ClamAV,
# ибо - ПО должно быть свободным! :)
# Итак, указываем местоположение сокета clamd.
acl_smtp_data = acl_check_data
```

```
av_scanner = clamd:/var/run/clamav/clamd.sock

# Адрес куда слать на проверку спама (SpamAssasin), но я
# это не юзаю. Не так много у меня спама...
#spamd_address = 127.0.0.1 783

# SSL
tls_certificate = /etc/ssl/certs/dovecot.pem
tls_privatekey = /etc/ssl/private/dovecot.pem

# Отключаем IPv6
disable_ipv6

#порт smtp
daemon_smtp_ports = 25 : 465
tls_on_connect_ports = 465

# Дописываем домены отправителя и получателя, если они не
указаны
qualify_domain = tst-amo.pp.ua
qualify_recipient = tst-amo.pp.ua

allow_domain_literals = false
exim_user = mailnull
exim_group = mail

never_users = root

# Проверять прямую и обратную записи узла отправителя по DNS
# Тока зачем это нужно - даже и незнаю... Спам на этом не
режется...
# Зато возможны проблемы - если сервер зоны скажет `сервер
файлед`
# то почту от этого хоста Вы не получите :)
#host_lookup = *

# Отключаем проверку пользователей узла отправителя по
протоколу ident
# * то будет проверять все
# identd - он может ответить (а может и не ответить - как
# настроить), скажет UID пользователя от которого установлено
```

```
# соединение, тип ОС, и имя пользователя. Теперь, понимаете,
почему
# у всех оно зарублено и файрволлами позакрыто?
#rfc1413_hosts = *
rfc1413_query_timeout = 0s

# Запрещаем использовать знак % для явной маршрутизации почты
# Позволяет выполнять что-то типа - пришло сообщение на
# локальный ящик user%test.su@lissyara.su и
# переправляет его на user@test.su. Делается это для
# перечисленного списка доменов (* - все)
#percent_hack_domains =

# Настройки обработки ошибок доставки, используются значения
по умолчанию
# Если сообщение было недоставлено, то генерится соощение
# об ошибке. Если сообщение об ошибке не удалось доставить
# то оно замораживается на указанный в этом пункте срок,
# после чего снова попытка доставить его. При очередной
# неудаче - сообщение удаляется.
ignore_bounce_errors_after = 2h
timeout_frozen_after = 14d

# Список хостов, почта от которых принимается, несмотря
# на ошибки в HELO/EHLO (тут указана моя подсеть)
helo_accept_junk_hosts = 192.168.1.0/24

# Через какое время повторять попытку доставки
# замороженного сообщения
auto_thaw = 1h

# Приветствие сервера
smtp_banner = "$primary_hostname, ESMTP EXIM $version_number"
#smtp_banner = "$primary_hostname, SUPER-PUPER MAIL SERVER"

# Максимальное число одновременных подключений по
# SMTP. Рассчитывать надо исходя из нагрузки на сервер
smtp_accept_max = 50

# максимальное число сообщений принимаемое за одно соединение
# от удалённого сервера (или пользователя). С числом 25
```

```
# я имел проблемы тока один раз - когда у меня три дня лежал
# инет и после его подъёма попёрли мессаги. Но у меня не так
# много почты - всего 30 пользователей.
smtp_accept_max_per_connection = 45

# чё-то про логи и борьбу с флудом - я так понимаю -
# максимальное число сообщений записываемых в логи
smtp_connect_backlog = 30

# максимальное число коннектов с одного хоста
smtp_accept_max_per_host = 20

# Ход ладьёй - для увеличения производительности,
# директория `spool` внутри, разбивается на
# директории - это ускоряет обработку
split_spool_directory = true

# Если у сообщения много адресатов на удалённых хостах,
# то запускатеся до указанного числа максимально число
# параллельных процессов доставки
remote_max_parallel = 15

return_size_limit = 10K

# разрешаем неположенные символы в HELO (столкнулся
# с этим случайно - имя фирмы состояло из двух слов
# и какой-то раздолбай домен обозвал my_firme_name
# прям с подчёркиваниями... Виндовые клиенты при
# соединении радостно рапортовали о себе
# `vasya.my_firme_name` ну а экзим их футболил :))
helo_allow_chars = _

syslog_timestamp = no

# Лимит размера сообщения (50 мегабайт default)
message_size_limit = 1000M

################
### конфигурация ACL для входящей почты
begin acl
```

```
# Эти правила срабатывают для каждого получателя

acl_check_rcpt:

# принимать сообщения которые пришли с локалхоста,
# не по TCP/IP

accept hosts = :

# Запрещаем письма содержащие в локальной части
# символы @; %; !; /; |. Учтите, если у вас было
# `percent_hack_domains` то % надо убрать.
# Проверяются локальные домены

deny message = "incorrect symbol in address"
 domains = +local_domains
 local_parts = ^[.] : ^.*[@%!/|]

# Проверяем недопустимые символы для
# нелокальных получателей:

deny message = "incorrect symbol in address"
 domains = !+local_domains
 local_parts = ^[./|] : ^.*[@%!] : ^.*/\\.\\./

# Принимаем почту для постмастеров локальных доменов без
# проверки отправителя (я закомментировал, т.к. это -
# основной источник спама с мой ящик).

accept local_parts = postmaster
 domains = +local_domains

# Запрещщаем, если невозможно проверить отправителя
# (отсутствует в списке локальных пользователей)
# У себя я это закоментил, по причине, что некоторые
# железяки (принтеры, & etc) и программы (Касперский, DrWEB)
# умеют слать почту, в случае проблем но не умеют ставить
# нужного отправителя. Такие письма эта проверка не пускает.
# require verify = sender

# Запрещаем тех, кто не обменивается приветственными
```

```
# сообщениями (HELO/EHLO)

deny message = "HELO/EHLO require by SMTP RFC"
 condition = ${if eq{$sender_helo_name}{}{yes}{no}}

# Принимаем сообщения от тех, кто аутентифицировался:
# Вообще, большинство конфигов в рунете - это один и тот же
# конфиг написанный Ginger, в котором этот пункт расположен
# внизу. Но при таком расположении рубятся клиенты с adsl,
# ppp, и прочие зарезанные на последующих проверках. Но это
# ж неправильно! Это мои пользователи из дома! Потому
# я это правило расположил до проверок.

accept authenticated = *

# Рубаем нах, тех, кто подставляет свой IP в HELO
deny message = "Your IP in HELO - access denied!"

hosts = * : !+relay_from_hosts : !81-196.lissyara.su
 condition = ${if eq{$sender_helo_name}\
 {$sender_host_address}{true}{false}}

# Рубаем тех, кто в HELO пихает мой IP (2500 мудаков за
месяц!)
deny condition = ${if eq{$sender_helo_name}\
 {$interface_address}{yes}{no}}
 hosts = !127.0.0.1 : !localhost : *
 message = "main IP in your HELO! Access denied!"

# Рубаем тех, кто в HELO пихает только цифры
# (не бывает хостов ТОЛЬКО из цифр)
deny condition = ${if match{$sender_helo_name}\
 {\N^\d+$\N}{yes}{no}}
 hosts = !127.0.0.1 : !localhost : *
 message = "can not be only number in HELO!"

# Рубаем хосты типа *adsl*; *dialup*; *pool*;....
# Нормальные люди с таких не пишут. Если будут
# проблемы - уберёте проблемный пункт (у меня клиенты
# имеют запись типа asdl-1233.zone.su - я ADSL убрал...)
deny message = "your hostname is bad (adsl, poll, ppp & etc)."
```

```
 condition = ${if match{$sender_host_name} \
 {adsl|dialup|pool|peer|dhcp} \
 {yes}{no}}
# Задержка. (это такой метод борьбы со спамом,
# основанный на принципе его рассылки) На этом рубается
# почти весь спам. Единственно - метод неприменим на
# реально загруженных MTA - т.к. в результате ему
# приходится держать много открытых соединений.
# но на офисе в сотню-две человек - шикарный метод.
#
# более сложный вариант, смотрите в статье по exim и
# курьер имап. Т.к. там метод боле умный (просто правил
# больше :), то можно и на более загруженные сервера ставить)

warn
# Ставим дефолтовую задержку в 30 секунд
 set acl_m0 = 0s

warn
# ставим задержку в 0 секунд своим хостам и
# дружественным сетям (соседняя контора :))
 hosts = +relay_from_hosts:192.168.1.0/24:194.44.219.160/28
 set acl_m0 = 0s
warn
# пишем в логи задержку (если оно вам надо)
 logwrite = Delay $acl_m0 for $sender_host_name \
 [$sender_host_address] with HELO=$sender_helo_name. Mail \
 from $sender_address to $local_part@$domain.
 delay = $acl_m0

# Проверка получателя в локальных доменах.
# Если не проходит, то проверяется следующий ACL,
# и если непрошёл и там - deny
accept domains = +local_domains
 endpass
 message = "In my mailserver not stored this user"
 verify = recipient

# Проверяем получателя в релейных доменах
# Опять-таки если не проходит -> следующий ACL,
# и если непрошёл и там - deny
```

```
accept domains = +relay_to_domains
 endpass
 message = "main server not know how relay to this address"
 verify = recipient

# Рубаем тех, кто в блэк-листах. Серваки перебираются
# сверху вниз, если не хост не найден на первом, то
# запрашивается второй, и т.д. Если не найден ни в одном
# из списка - то почта пропускается.
deny message = you are in blacklist: $dnslist_domain -->
$dnslist_text
 dnslists = opm.blitzed.org : \
 # cbl.abuseat.org : \
 # bl.csma.biz : \
 dynablock.njabl.org

# Разрешаем почту от доменов в списке relay_from_hosts
accept hosts = +relay_from_hosts

# Если неподошло ни одно правило - чувак явно ищет
# открытый релей. Пшёл прочь. :)
deny message = "relay not permitted"

###############
# Проверка вложений
acl_check_mime:
deny message = Это сообщение содержит опасное вложение
 condition = ${if match{$mime_filename}{\N(?i)\.zip$\N}}
 decode = default
  condition  =  ${if  match{${run{/usr/bin/unzip  -l
$mime_decoded_filename}}}{\N(?i)\.(exe|com|vbs|bat|pif|scr|hta
|js|cmd|chm|cpl|jsp|reg|vbe|lnk|dll|sys)\n\N}}
 log_message = forbidden attachment: filename=$mime_filename,
content-type=$mime_content_type, recipients=$recipients

deny message = Это сообщение содержит опасное вложение
 condition = ${if match{$mime_filename}{\N(?i)\.rar$\N}}
 decode = default
  condition  =  ${if  match{${run{/usr/bin/unrar  l
$mime_decoded_filename}}}{\N(?i)\.(exe|com|vbs|bat|pif|scr|hta
|js|cmd|chm|cpl|jsp|reg|vbe|lnk|dll|sys)\n\N}}
```

```
 log_message = forbidden attachment: filename=$mime_filename,
content-type=$mime_content_type, recipients=$recipients
accept

#########

# Тут идут ACL проверяющие содержимое (тело) письма.
# Без них будут пропускаться все сообщения.

acl_check_data:

# Заблокированные аккаунты
 deny senders = /usr/local/etc/exim/deny_senders
 message = "DENY!!! Your address is: $sender_address in the
black list!!!"
  #  logwrite  =  Rejected  from  $sender_address  to
$local_part@$domain by blacklist.
  log_message  =  Rejected  from  $sender_address  to
$local_part@$domain by blacklist.

# Проверка на вирусы
 deny message = In email found VIRUS ($malware_name)
 malware = *

# accept by default
 accept

###############
begin routers

check_malware:
 driver = redirect
 condition = ${if def:h_X-Quarantine-Me-Malware: {1}{0}}
 headers_remove = Subject
 headers_add = Subject: [CLAMAV: $acl_m2] $h_Subject
 data = postmaster@tst-amo.pp.ua
 file_transport = address_file

# Поиск маршрута к хосту в DNS. Если маршрут не найден в DNS -
# то это `унроутабле аддресс`. Не проверяются локальные
# домены, 0.0.0.0 и 127.0.0.0/8
```

```
dnslookup:
 driver = dnslookup
 domains = ! +local_domains
 transport = remote_smtp
 ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
 no_more

# Смотрим алиасы
system_aliases:
 driver = redirect
 allow_fail
 allow_defer
 data = ${lookup mysql{SELECT `goto` FROM `alias` WHERE \
 `address`='${quote_mysql:$local_part@$domain}' OR \
 `address`='${quote_mysql:@$domain}'}}

# Те, что находятся /etc/mail/aliases

system_aliases2:
 driver = redirect
 allow_fail
 allow_defer
 data = ${lookup{$local_part}lsearch{/etc/aliases}}
 user = mailnull
 group = mail
 file_transport = address_file
 pipe_transport = address_pipe

# DSPAM ROUTERS
dspam_addspam_router:
 driver = accept
 domains = +local_domains
 local_part_prefix = spam-
 transport = dspam_addspam_transport

dspam_notspam_router:
 driver = accept
 domains = +local_domains
 local_part_prefix = notspam-
 transport = dspam_notspam_transport
```

```
dspam_spamscan_router:
 driver = accept
 domains = +local_domains
 no_verify
  condition = "${if and {{!eq {$received_protocol}{spam-
scanned}} \
 {!eq {$received_protocol}{local}} } {1}{0}}"
 transport = dspam_spamcheck_transport
 require_files = /usr/local/bin/dspam
 address_test = false
 user = mailnull
 group = mail

local_delivery_spam_router:
 driver = accept
 domains = +local_domains
 condition = ${if match{$h_X-DSPAM-Result:}{Spam}}
 transport = local_delivery_spam_transport
 no_more
 user = mailnull
 group = mail

# LOCAL DELIVERY
# Роутер для вирт польз MySQL
dovecot_user:
 driver = accept
 condition = ${lookup mysql{SELECT `goto` FROM \
 `alias` WHERE \
 `address`='${quote_mysql:$local_part@$domain}' OR \
 `address`='${quote_mysql:@$domain}'}{yes}{no}}

transport = dovecot_delivery
 cannot_route_message = Unknown user

# Роутер для системных
#localuser2:
# driver = accept
# check_local_user
# #transport = dovecot_delivery
# transport = local_delivery
# transport_current_directory = /
```

```
# cannot_route_message = Unknown user

##################
begin transports

remote_smtp:
 driver = smtp

# DSPAM TRANSPORT
dspam_addspam_transport:
 driver = pipe
 command = "/usr/local/bin/dspam --user \
 $local_part@$domain --class=spam --source=error"
 return_path_add = false
 return_fail_output = true
 log_output = true
 home_directory = "/var/db/dspam"
 current_directory = "/var/db/dspam"
 user = mailnull
 #user = dspam
 group = mail

dspam_notspam_transport:
 driver = pipe
 command = "/usr/local/bin/dspam --user \
 $local_part@$domain --class=innocent \
 --source=error --deliver=innocent %u"
 return_path_add = false
 return_fail_output = true
 log_output = true
 home_directory = "/var/db/dspam"
 current_directory = "/var/db/dspam"
 #user = dspam
 user = mailnull
 group = mail

dspam_spamcheck_transport:
 driver = pipe
 command = /usr/local/bin/dspam --deliver=innocent \
 --user "$local_part@$domain" -- %u
```

```
#user = dspam
 user = mailnull
 group = mail
 return_path_add = false
 log_output = true
 return_fail_output = true
 headers_remove = X-DSPAM-Result

local_delivery_spam_transport:
 driver = pipe
# Команда перемещения писем распознанных как спам в каталог спама
# у меня этот каталог Junk
 command = /usr/local/libexec/dovecot/deliver -d \
 $local_part@$domain -m Junk
 message_prefix =
 message_suffix =
 delivery_date_add
 envelope_to_add
 return_path_add
 log_output
 user = mailnull
 group = mail

# Транспорт для виртуальных получателей из Dovecot (MySQL)
dovecot_delivery:
 driver = pipe
  command = /usr/local/libexec/dovecot/dovecot-lda -e -d $local_part@$domain -f $sender_address -a $original_local_part@$original_domain
 return_path_add
 log_output = true
 delivery_date_add
 envelope_to_add
 user = mailnull
 group = mail
 return_output

# Транспорт для системных пользователей
# Does not work sieve!
#local_delivery:
```

```
# driver = appendfile
# maildir_format
# maildir_tag = ,S=$message_size
## directory = /home/mail/$domain/$local_part
# directory = /var/vmail/$local_part/Maildir
# create_directory
# delivery_date_add
# envelope_to_add
# return_path_add
# group = mail
# mode = 0660
# no_mode_fail_narrower

address_pipe:
 driver = pipe
 return_output

address_file:
 driver = appendfile
 delivery_date_add
 envelope_to_add
 return_path_add

address_reply:
 driver = autoreply

begin retry
* * F,2h,15m; G,16h,1h,1.5; F,4d,6h

begin rewrite

###############
begin authenticators

# Для системных пользователей через EXIM
#LOGIN:
# driver = plaintext
# public_name = LOGIN
# server_prompts = "Username:: : Password::"
# server_condition = "${if pam {$auth1:$auth2}{yes}{no}}"
# server_set_id = $auth1
```

```
#PLAIN:
# driver = plaintext
# public_name = PLAIN
# server_condition = "${if pam {$auth2:$auth3}{yes}{no}}"
# server_set_id = $auth2


# Аутентификация через dovecot
dovecot_login:
driver = dovecot
public_name = LOGIN
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1

dovecot_plain:
driver = dovecot
public_name = PLAIN
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1

dovecot_cram_md5:
driver = dovecot
public_name = CRAM-MD5

server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1

#########################

2. Ставим dovecot

cd /usr/ports/mail/dovecot2
make install clean
```