Exim - настройка вторичного mail exchanger

Опубликовано muff в Вс, 2015-07-19 00:00

Переносил вторичный **mail exchanger (MX)** на новый сервер. Решил выложить инфу и конфиги - еще пригодится...

Исходные данные:

- Hostname: **mx2.kyivlink.com**
- IP: **195.12.59.26**
- Domain: **kyivlink.com**

Проверяем, куда указывают записи **mail exchanger** домена **kyivlink.com** (сервер мультидоменный, но тестировать будем на этом домене):

```
# host -t mx kyivlink.com
kyivlink.com mail is handled by 10 mail.kyivlink.com.
kyivlink.com mail is handled by 20 mx2.kyivlink.com.
```

Важно! Необходимо, чтобы "прямая" и "обратная" запись в **DNS** совпадали. Тоесть в нашем случае, необходимо чтобы запись **mx2.kyivlink.com** "резолвилась" в IP-адрес **195.12.59.26**, а **PTR**-запись для IP **195.12.59.26** была установлена в **mx2.kyivlink.com**.

Проверим, выполняются ли эти условия:

```
# host mx2.kyivlink.com.
mx2.kyivlink.com has address 195.12.59.26

# host 195.12.59.26
26.59.12.195.in-addr.arpa domain name pointer mx2.kyivlink.com.
```

В **DNS**-записях все в порядке. Приступим непосредственно к настройке **Exim**.

Внесем в **/etc/make.conf** следующий блок:

```
PORTSDIR?= /usr/ports
# EXIM
.if ${.CURDIR} == ${PORTSDIR}/mail/exim
LOG_FILE_PATH?= syslog
WITH_DEFAULT_CHARSET?= koi8-r
.endif
```

Виполним установку **Exim** из системы портов:

```
# cd /usr/ports/mail/exim && make install clean && rehash
```

При сборке указываем необходимость сборки с поддержкой **MySQL**:

```
[x] MYSQL           Enable mysql lookups
[x] SPF             Enable Sender Policy Framework checking
```

По завершению установки выводится список рекомендуемых действий:

```
To use Exim instead of sendmail on startup:

*) Clear the sendmail queue and stop the sendmail daemon.
*) Adjust mailer.conf(5) as appropriate.
*) Set the 'sendmail_enable' rc.conf(5) variable to 'NONE'.
*) Set the 'daily_status_include_submit_mailq' and
   'daily_clean_hoststat_enable' periodic.conf(5)
   variables to 'NO'.
*) Consider setting 'daily_queuerun_enable' and
   'daily_submit_queuerun' to "NO" in periodic.conf(5),
   if you intend to manage queue runners / deliveries closely.
*) Set the 'exim_enable' rc.conf(5) variable to 'YES'.
*) Start exim with '/usr/local/etc/rc.d/exim start'.

You may also want to configure newsyslog(8) to rotate Exim log files:

/var/log/exim/mainlog   mailnull:mail 640 7 * @T00 ZN
/var/log/exim/rejectlog mailnull:mail 640 7 * @T00 ZN
```

Относительно настройки ротации логов (в конце рекомендаций) - можно пропустить этот пункт, поскольку в опциях сборки указывали, что логировние будет выполняться с помощью **syslog**, тоесть логирование будет выполняться в **maillog**, настройка ротации которого уже выполнена.

А вот остальные рекомендации стоит выполнить.

Останавливаем **sendmail** и отключаем его поддержку в **rc.conf**:

```
# sh /etc/rc.d/sendmail forcestop
# echo '# Disable Sendmail' >> /etc/rc.conf
# echo 'sendmail_enable="NONE"' >> /etc/rc.conf
```

Файл **/etc/mail/mailer.conf** приводим к следующему состоянию:

```
sendmail        /usr/local/sbin/eximsend-mail       /usr/local/sbin/eximmailq
    /usr/local/sbin/exim -bpnewaliases      /usr/local/sbin/exim -bihoststat
/usr/local/sbin/eximpurgestat       /usr/local/sbin/exim
```

Настраиваем **periodic.conf**:

```
# echo 'daily_status_include_submit_mailq="NO"' >> /etc/periodic.conf
# echo 'daily_clean_hoststat_enable="NO"' >> /etc/periodic.conf
# echo 'daily_queuerun_enable="NO"' >> /etc/periodic.conf
# echo 'daily_submit_queuerun="NO"' >> /etc/periodic.conf
```

Остается только добавить поддержку **Exim** в **rc.conf** и запустить **Exim**. Однако, предварительно необходимо его настроить.

Отталкиваемся от того, что MySQL **[1]** и **Clamav** [2] установлены, настроены и работают.

Отредактируем **/usr/local/etc/exim/configure** до следующего содержания:

```
######################################################################
     Runtime configuration file for Exim                ###############################
```

```
##########################################################################
############################                    MAIN CONFIGURATION SETTINGS
                ##########################################################################
GREYLIST_ENABLED_GREY        = yesGREYLIST_INITIAL_DELAY       = 15 MINUTEGREYLIS
T_INITIAL_LIFETIME      = 4 HOURGREYLIST_WHITE_LIFETIME       = 12 DAYGREYLIST_BOU
NCE_LIFETIME      = 7 DAYGREYLIST_RECORD_LIFETIME      = 30 DAYGREYLIST_TABLE
        = greylist.ifdef GREYLIST_ENABLED_GREY   GREYLIST_TEST = SELECT CASE \   WHE
N now() > block_expires THEN "accepted" \   ELSE "deferred" \   END AS result, id \   FRO
M GREYLIST_TABLE \   WHERE (now() < record_expires) \   AND (sender_type = ${if def:se
nder_address_domain{'NORMAL'}{'BOUNCE'} }) \   AND (sender = '${quote_mysql:${if d
ef:sender_address_domain{$sender_address_domain}{${domain:$h_from:}} }}') \   AND
 (recipient = '${quote_mysql:${if def:domain{$domain}{${domain:$h_to:}} }}') \   AND
(relay_ip = '${quote_mysql:${mask:$sender_host_address/32}}') \   ORDER BY result DES
C LIMIT 1GREYLIST_ADD = REPLACE INTO GREYLIST_TABLE \   (relay_ip, sender_type, sen
der, recipient, block_expires, \   record_expires, create_time, type) \   VALUES ( '${quote_
mysql:${mask:$sender_host_address/32}}', \   ${if def:sender_address_domain{'NORMA
L'}{'BOUNCE'}}, \   '${quote_mysql:${if def:sender_address_domain{$sender_address_d
omain}{${domain:$h_from:}} }}', \   '${quote_mysql:${if def:domain{$domain}{${dom
ain:$h_to:}} }}', \   DATE_ADD(now(), INTERVAL GREYLIST_INITIAL_DELAY), \   DATE_ADD(
now(), INTERVAL GREYLIST_INITIAL_LIFETIME), \   now(), \   'AUTO' \   )   GREYLIST_DEFER
_HIT = UPDATE GREYLIST_TABLE \   SET blockcount=blockcount+1, last_block=now() \   W
HERE id = $acl_m9   GREYLIST_OK_COUNT = UPDATE GREYLIST_TABLE \   SET passcount=
passcount+1, last_pass=now() \   WHERE id = $acl_m9   GREYLIST_OK_NEWTIME = UPDAT
E GREYLIST_TABLE \   SET record_expires = DATE_ADD(now(), INTERVAL GREYLIST_WHITE
_LIFETIME) \   WHERE id = $acl_m9 AND type='AUTO'   GREYLIST_OK_BOUNCE = UPDATE G
REYLIST_TABLE \   SET record_expires = DATE_ADD(now(), INTERVAL GREYLIST_BOUNCE_L
IFETIME) \   WHERE id = $acl_m9 AND type='AUTO'   GREYLIST_CLEAN = DELETE FROM GR
EYLIST_TABLE \   WHERE (DATE_ADD(record_expires, INTERVAL GREYLIST_RECORD_LIFETI
ME) < now()) AND (type='AUTO').endifprimary_hostname = mx2.kyivlink.com
domainlist local_domains = ${lookup mysql{SELECT domain FROM domains \
   WHERE domain='${domain}' AND \                    (type='LOCAL' OR type='VIRTUAL')}
}domainlist relay_to_domains = ${lookup mysql{SELECT domain FROM domains \
        WHERE domain='${domain}' AND type='RELAY'}}hostlist spamers = ${lookup my
sql{SELECT senders FROM blacklist_host WHERE senders='${sender_host_address}'}}ho
stlist relay_from_hosts = localhostauth_advertise_hosts = *daemon_smtp_ports = 25log_s
elector = \       +all_parents \       +lost_incoming_connection \       +received_sender \
  +received_recipients \       +smtp_confirmation \       +smtp_syntax_error \       +smtp_
protocol_error \       -queue_runacl_smtp_rcpt = acl_check_rcptacl_smtp_data = acl_check_
dataav_scanner = clamd:/var/run/clamav/clamd.sockqualify_domain = mx2.kyivlink.com
local_interfaces = 195.12.59.26
allow_domain_literals = falseexim_user = mailnullexim_group = mailnever_users = rootho
st_lookup = *rfc1413_hosts = *rfc1413_query_timeout = 5ssyslog_duplication = falseigno
re_bounce_errors_after = 5dtimeout_frozen_after = 7dmessage_size_limit = 20Mrecipient
s_max = 50smtp_accept_max = 150smtp_accept_max_per_connection = 20smtp_accept_m
ax_per_host = 20smtp_connect_backlog = 50smtp_accept_queue_per_connection = 30spli
t_spool_directory = trueremote_max_parallel = 15smtp_banner = "MX2.KYIVLINK.COM
 ESMTP"hide mysql_servers = localhost/exim/exim/MYSQL_PASS_HERE
##########################################################
############                    ACL CONFIGURATION                    ##       Specifies ac
cess control lists for incoming SMTP mail      ###################################
#############################################
begin acl.ifdef GREYLIST_ENABLED_GREY greylist_acl:
# clean greylist records as 09:3xBRST 10:3xBRDT (horario normal)
  warn  condition  = ${if eq {${substr{8}{4}{$tod_zulu} }} {0100}{yes}{no}}       set
acl_m4 = ${lookup mysql{GREYLIST_CLEAN}}
  # For regular deliveries, check greylist.  # check greylist tuple, returning "accepted", "
deferred" or "unknown"  # in acl_m8, and the record id in acl_m9
  warn set acl_m8 = ${lookup mysql{GREYLIST_TEST}{$value}{result=unknown}}
# here acl_m8 = "result=x id=y"
```

```
     set acl_m9 = ${extract{id}{$acl_m8}{$value}{-1}}
# now acl_m9 contains the record id (or -1)
     set acl_m8 = ${extract{result}{$acl_m8}{$value}{unknown}}
# now acl_m8 contains unknown/deferred/accepted
# check if we know a certain triple, add and defer message if not  accept
# if above check returned unknown (no record yet)
     condition = ${if eq {$acl_m8} {unknown} {1}}      # then also add a record
     condition = ${lookup mysql{GREYLIST_ADD}{yes}{no}}
# check if the triple is still blocked  accept
# if above check returned deferred then defer
     condition = ${if eq{$acl_m8} {deferred} {1}}      # and note it down
     condition = ${lookup mysql{GREYLIST_DEFER_HIT}{yes}{yes}}
# use a warn verb to count records that were hit
 warn condition = ${lookup mysql{GREYLIST_OK_COUNT}}
# use a warn verb to set a new expire time on automatic records,  # but only if the mail was not a bounce, otherwise set to now().
 warn !senders = : postmaster@* : Mailer-Daemon@*      condition = ${lookup mysql{GREYLIST_OK_NEWTIME}}  warn senders = : postmaster@* : Mailer-Daemon@*      condition = ${lookup mysql{GREYLIST_OK_BOUNCE}}  deny.endifacl_check_rcpt:  accept  hosts = +relay_from_hosts  deny    domains       = +local_domains          local_parts   = ^[.] : ^.*[@%!/|]  deny    domains       = !+local_domains                local_parts   = ^[./|] : ^.*[@%!] : ^.*/\\.\\./  accept  local_parts   = postmaster         domains       = +local_domains  deny    message       = HELO/EHLO required by SMTP RFC         condition     = ${if eq{$sender_helo_name}{}{yes}{no}}# orange.fr war :)
 deny    message         = all email from *.orange.fr - discarded!         condition       = ${if match{$sender_helo_name}{.orange.fr}{yes}{no}}# .bezeqint.net
 deny    message         = all email from *.bezeqint.net - discarded!         condition       = ${if match{$sender_helo_name}{.bezeqint.net}{yes}{no}}# .libero.it
 deny    message         = all email from *.libero.it - discarded!         condition       = ${if match{$sender_helo_name}{.libero.it}{yes}{no}}# .ono.com
 deny    message         = all email from *.ono.com - discarded!         condition       = ${if match{$sender_helo_name}{.ono.com}{yes}{no}}# isp.novis.pt
 deny    message         = all email from *.isp.novis.pt - discarded!         condition       = ${if match{$sender_helo_name}{.isp.novis.pt}{yes}{no}}  deny   message= Yoy address in banlist!         senders=${lookup mysql{SELECT senders FROM blacklist WHERE senders='${quote_mysql:$sender_address}' \         OR senders='*@${quote_mysql:$sender_address_domain}' LIMIT 1}}  deny    hosts = +spamers         message       = Host rejected by: spamers list on rbl.mx2.kyivlink.com
.  deny    message       = Go Away! You are spammer.          condition     = ${if match{$sender_host_name} \                    {bezeqint\\.net|net\\.il|dialup|pool|peer|ppp|dhcp} \                    {yes}{no}}  deny    message       = rejected because $sender_host_address \         is in a black list at $dnslist_domain\n$dnslist_text         hosts         = !+relay_from_hosts         !authenticated = *         log_message   = found in $dnslist_domain         dnslists      = bl.spamcop.net : \                    cbl.abuseat.org : \                    dnsbl.njabl.org : \                    sbl-xbl.spamhaus.org : \
   pbl.spamhaus.org  drop    message     = Rejected - Sender Verify Failed         log_message = Rejected - Sender Verify Failed                    !verify = sender/no_details/callout=2m,defer_ok
      !condition =  ${if eq{$sender_verify_failure}{}}   .ifdef GREYLIST_ENABLED_GREY    defer hosts         = !+relay_from_hosts         !authenticated = *         !senders       = : postmaster@* : Mailer-Daemon@*         acl           = greylist_acl         message       = GreyListed: please try again later   .endif  accept  domains       = +local_domains          endpass          message       = unknown user          verify        = recipient  accept  domains       = +relay_to_domains         endpass          message       = Unknown user          verify        = recipient/callout=2m,defer_ok,use_postmaster  accept  hosts      = +relay_from_hosts  accept  authenticated = *  deny    message       = relay not permittedaccep tacl_check_data:  .ifdef GREYLIST_ENABLED_GREY    defer hosts         = !+relay_from_hosts         senders         = : postmaster@* : Mailer-Daemon@*         acl           = greylist_acl         message         = GreyListed: please try again later  .endifdeny     message  = This message contains a virus ($malware_name).         demime    = *         malware   = */defer_okaccept
##########################################################################################                    ROUTERS CONFIGURATION                    ##               Specifies how addresses are handled                ######################################
```

```
##################################     THE ORDER IN WHICH THE ROUTERS AR
E DEFINED IS IMPORTANT!      ## An address is passed to each router in turn until it is accepted.  #
##################################################################
##########
begin routersdnslookup:  driver = dnslookup  domains = ! +local_domains  transport = remote_smt
p  ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8  no_moresystem_aliases:  driver = redirect  allow_fail
allow_defer  data = ${lookup mysql{SELECT recipients FROM aliases \        WHERE (local_part='${l
ocal_part}' AND domain='${domain}') \        OR (local_part='*' AND domain='$domain')ORDER BY l
ocal_part='*' LIMIT 1}}virtual_localuser:  driver = accept  domains = ${lookup mysql{SELECT doma
in from domains WHERE domain='${domain}'}}  local_parts = ${lookup mysql{SELECT login from
users \            WHERE login='${local_part}' AND domain='${domain}'}}  transport = local_deliver
y  cannot_route_message = Unknown user
##################################################################
##########                  TRANSPORTS CONFIGURATION                  ##############
##################################################################
              ORDER DOES NOT MATTER                    ##     Only one appropriate transport is called f
or each delivery.    ##################################################
#########################begin transportsremote_smtp:  driver = smtp  interface =
195.12.59.26
local_delivery:  driver = appendfile  check_string = ""  create_directory  delivery_date_add  directory
 = ${lookup mysql{SELECT LOWER(CONCAT('/var/exim/$domain/',login)) FROM users \              WH
ERE login='${local_part}' AND domain='${domain}';}}  directory_mode = 770  envelope_to_add  g
roup = mail  maildir_format  maildir_tag = ,S=$message_size  message_prefix = ""  message_suffix
= ""  mode = 0660  quota = ${lookup mysql{SELECT quota FROM users \        WHERE login='${loc
al_part}' AND domain='${domain}'}{${value}M}}  quota_size_regex = S=(\d+)$  quota_warn_thre
shold = 75%  return_path_addaddress_pipe:   driver = pipe   return_outputaddress_file:  driver = ap
pendfile  delivery_date_add  envelope_to_add  return_path_addaddress_reply:  driver = autoreply
##################################################################
##########                  RETRY CONFIGURATION                  ###############
##################################################################
begin retry*                  quota*                  *         F,2h,15m; G,16h,1h,1.5; F,4d,6h
##################################################################
##########                  REWRITE CONFIGURATION                  ###############
##################################################################
begin rewrite
##################################################################
##########                AUTHENTICATION CONFIGURATION                ############
##################################################################
begin authenticators# End of Exim configuration file
```

Создадим базу данных **MySQL** и пользователя с правами на эту БД:

```
mysql> create database exim;
Query OK, 1 row affected (0,00 sec)

mysql> grant all on exim.* to 'exim'@'localhost' identified by 'MYSQL_PASS_HERE';
Query OK, 0 rows affected (0,00 sec)
```

Скачиваем дамп и заливаем его в БД:

```
# fetch http://muff.kiev.ua/files/exim_mx2.sql
# mysql -u exim -pMYSQL_PASS_HERE exim < exim_mx2.sql
```

Внимание! В моем случае, дамп БД готов для использования. Если же использовать на других серверах, необходимо изменить данные (можно и структуру, например, дефолтные значения) в таблицах **aliases** и **domains**.

Запускаем **exim**:

```
# sh /usr/local/etc/rc.d/exim start
```

Проверяем, запустился ли демон:

```
# ps -ax | grep exim
70442  -  Is       0:00,00 /usr/local/sbin/exim -bd -q30m
```

Демон запустился. Настройка **Exim** в роли вторичного **mail exchanger (MX)** завершена.

Источник (получено *2025-07-04 01:13*):
http://muff.kiev.ua/content/exim-nastroika-vtorichnogo-mail-exchanger

Ссылки:
[1] http://muff.kiev.ua/content/mysql-ustanovka-i-bazovaya-nastroika
[2] http://muff.kiev.ua/content/clamav-antivirusnaya-zashchita-servera