

Почтовый сервер Exim + Dovecot

Опубликовано вс, 12/15/2013 – 18:26 пользователем Demontager

Заметка о том как можно настроить самый простой почтовый сервер на базе Exim и Dovecot. Этот конфиг я использовал на FreeBSD сервере и только модифицировал его чтобы он работал на Debian/Ubuntu Linux. Используется *простая SMTP авторизация с хранением аккаунтов и паролей в базе данных MySQL*. Так как мне не нужно защищенное соединение, *SSL/TLS авторизация не используется*. Пошагово разберем установку

1. Начнем с установки пакетов

```
#apt-get install dovecot-imapd dovecot-pop3d dovecot-common  
dovecot-mysql exim4-daemon-heavy
```

2. Ставим mysql сервер и задаем пароль рута

```
apt-get install mysql-server  
mysqladmin -u root password NEWPASSWORD
```

3. Создать БД exim_db.

```
mysql -uroot -pMySQLpass  
mysql>create database exim_db;  
mysql>quit;
```

Заранее подготовить структуру таблиц в базе mysql. Сохраните ее в формате base.sql в любом текстовом редакторе и подготовьте для импорта.

```
-- phpMyAdmin SQL Dump  
-- version 4.0.4-rc1  
-- http://www.phpmyadmin.net  
--  
-- Host: localhost  
-- Generation Time: Dec 15, 2013 at 03:08 PM  
-- Server version: 5.5.29-0ubuntu1  
-- PHP Version: 5.4.9-4ubuntu2  
SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";  
SET time_zone = "+00:00";
```

```

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT
*/;

                                /*!40101                                SET
@OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION
*/;
/*!40101 SET NAMES utf8 */;
--
-- Database: `exim_db`
--
-- -----
--
-- Table structure for table `accounts`
--
CREATE TABLE IF NOT EXISTS `accounts` (
  `login` varchar(128) COLLATE utf8_bin NOT NULL DEFAULT '',
  `password` varchar(128) COLLATE utf8_bin NOT NULL DEFAULT
'',
  `uid` int(11) NOT NULL DEFAULT '118',
  `gid` int(11) NOT NULL DEFAULT '8',
  `domain` varchar(128) COLLATE utf8_bin NOT NULL DEFAULT
'nixtalk.com',
  `quota` varchar(16) COLLATE utf8_bin NOT NULL DEFAULT
'250M',
  `status` int(11) NOT NULL DEFAULT '1',
  PRIMARY KEY (`login`,`domain`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
--
-- Dumping data for table `accounts`
--
INSERT INTO `accounts` (`login`, `password`, `uid`, `gid`,
`domain`, `quota`, `status`) VALUES
('support', 'secretPassword', 118, 8, 'nixtalk.com', '250M',
1);
--
-- -----
--
-- Table structure for table `aliases`
--
CREATE TABLE IF NOT EXISTS `aliases` (
  `address` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `goto` varchar(128) COLLATE utf8_bin DEFAULT NULL,

```

```

`domain` varchar(128) COLLATE utf8_bin DEFAULT 'nixtalk.com'
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
-- -----
--
-- Table structure for table `domains`
--
CREATE TABLE IF NOT EXISTS `domains` (
  `domain` varchar(128) COLLATE utf8_bin NOT NULL DEFAULT '',
  `status` int(11) NOT NULL DEFAULT '1',
  PRIMARY KEY (`domain`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
--
-- Dumping data for table `domains`
--
INSERT INTO `domains` (`domain`, `status`) VALUES
('nixtalk.com', 1);
-- -----
--
-- Table structure for table `whitelist`
--
CREATE TABLE IF NOT EXISTS `whitelist` (
  `senders` varchar(128) CHARACTER SET utf8 COLLATE utf8_bin
NOT NULL DEFAULT 'support@nixtalk.com'
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT
*/;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS
*/;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION
*/;

```

Пояснения к структуре базы:

для примера уже вставлен один аккаунт *support@nixtalk.com* с квотой *250M*. Если нужно добавить другой аккаунт, предпочтительно делать это в *phpmyadmin*, выбрав таблицу и нажав *Insert*. По дефолту доступ к почте имеет пользователь с *uid 118*, входящий в группу с *gid 8*.

Импортируем базу через *phpmyadmin* или с терминала

```
mysql -uroot -pMySQLpass exim_db < base.sql
```

4. Редактируем основной конфиг *exim-a*

```
nano /etc/exim4/update-exim4.conf.conf
```

```
#почта будет ходить через Internet
dc_eximconfig_configtype='internet'
dc_other_hostnames='nixtalk.com'
dc_local_interfaces='127.0.0.1'
dc_readhost=''
dc_relay_domains='nixtalk.com'
dc_minimaldns='false'
```

```
#через эти сети разрешен relay
dc_relay_nets='127.0.0.1:77.124.5.76'
dc_smarthost=''
CFILEMODE='644'
dc_use_split_config='false'
dc_hide_mailname=''
dc_mailname_in_oh='true'
dc_localdelivery='mail_spool'
dc_use_split_config='false'
```

— очень важный момент, этим мы указывает что хотим использовать *только один конфигурационный файл для exim*. Это сделано в целях удобства, так как общая конфигурация довольно простая и не требует указания большого количества директив. После внесения изменений не забываем выполнить

```
update-exim4.conf
```

Все файлы и папки кроме `update-exim4.conf.conf` и `exim4.conf.template` можно удалить. Теперь редактируем `exim4.conf.template`

```
nano /etc/exim4/exim4.conf.template
```

и приводим к такому виду, заменяя на свои данные

```
primary_hostname = mail.nixtalk.com
# имя базы и пароль
hide mysql_servers = localhost/exim_db/exim/eximPassword
domainlist local_domains = ${lookup mysql{select domain from
domains where domain='${domain}'}}
domainlist relay_to_domains = ${lookup mysql{select domain
from domains where domain='${domain}'}}
hostlist relay_from_hosts = localhost : 127.0.0.1
```

```

acl_smtp_rcpt = acl_check_rcpt
acl_smtp_data = acl_check_data
#tls_certificate = /etc/ssl/certs/favmail.pem
#tls_privatekey = /etc/ssl/certs/favmail.pem
#nopt smtp
daemon_smtp_ports = 25
#tls_on_connect_ports = 465
qualify_domain = mail.nixtalk.com
allow_domain_literals = false
exim_user = Debian-exim
exim_group = mail
never_users = root
host_lookup = *
rfc1413_hosts = *
rfc1413_query_timeout = 5s
ignore_bounce_errors_after = 2h
timeout_frozen_after = 7d
return_size_limit = 10K
split_spool_directory = true
syslog_timestamp = no

begin acl
acl_check_rcpt:
accept hosts = :
deny domains = +local_domains
    local_parts = ^[.] : ^.*[@%!/|]
deny domains = !+local_domains
    local_parts = ^[./|] : ^.*[@%!] : ^.*[/\\.\|\.|]
accept senders=${lookup mysql{SELECT senders FROM whitelist \
WHERE senders='${quote_mysql:$sender_address}'} }
deny message = HELO/EHLO required by SMTP RFC
    condition = ${if eq{$sender_helo_name}}{yes}{no}}
deny message = Go Away! You are spammer.
    condition = ${if match{$sender_host_name} \
        {bezeqint\\.net|net\\.il|pool|peer|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 : \
                 pbl.spamhaus.org

warn
    set acl_m0 = 25s

warn
    hosts = +relay_from_hosts
    set acl_m0 = 0s

warn
    authenticated = *
    set acl_m0 = 0s

warn
    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
drop    message      = Rejected - Sender Verify Failed
        log_message  = Rejected - Sender Verify Failed
        hosts        = *
        !verify       = sender/no_details/callout=2m,defer_ok
        !condition    = ${if eq{$sender_verify_failure}{}}

accept  domains      = +local_domains
        endpass
        message      = unknown user
        verify       = recipient

accept  domains      = +relay_to_domains
        endpass
        message      = unrouteable address
        verify       = recipient

accept  hosts        = +relay_from_hosts

accept  authenticated = *
deny    message      = relay not permitted

acl_check_data:
# China symbols

```

```

deny    message = This is spam - denied
        !senders = :
        condition = ${if match{$message_body}{105[-_]*51[-_]*86|778[-_]*98[-_]*94}{yes}{no}}

#Extensions
deny    message = contains $found_extension file (blacklisted).
        !senders = :
        demime = com:vbs:bat:pif:scr:exe

#Check MIME
deny    message = This message contains a MIME error
($demime_reason)
        !senders = :
        demime = *
        condition = ${if >{$demime_errorlevel}{2}{1}{0}}

#Messages with NUL- symbols
deny    message = This message contains NUL characters
        !senders = :
        log_message = NUL characters!
        condition = ${if >{$body_zerocount}{0}{1}{0}}

# Headers
deny    message = Incorrect headers syntax
        hosts = !+relay_from_hosts:*
        !senders = :
        !verify = header_syntax
accept

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

system_aliases:
    driver = redirect
    allow_fail

```

```

allow_defer
    data = ${lookup mysql{select goto from aliases where
address='${quote_mysql:$local_part}'                and
domain='${quote_mysql:$domain}'}}
    user = Debian-exim
    group = mail
    file_transport = address_file
    pipe_transport = address_pipe

userforward:
    driver = redirect
    check_local_user
    no_verify
    no_expn
    check_ancestor
    file_transport = address_file
    pipe_transport = address_pipe
    reply_transport = address_reply
    data = ${lookup mysql{select goto from aliases where
address='${quote_mysql:$local_part}'                and
domain='${quote_mysql:$domain}'}}

localuser:
    driver = accept
    domains = ${lookup mysql{select domain from domains where
domain='${domain}'}}
    local_parts = ${lookup mysql{select login from accounts
where login='${local_part}' and domain='${domain}'}}
    transport = local_delivery
    cannot_route_message = Unknown user

begin transports
remote_smtp:
    driver = smtp

local_delivery:
    driver = appendfile
    maildir_format
    maildir_tag = ,S=$message_size
    directory = /home/mail/$domain/$local_part
    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
```

```
auth_plain:
  driver                = plaintext
  server_set_id          = $2
  server_prompts         = :
  public_name            = PLAIN
  server_condition       = ${lookup mysql{select login
from accounts where login='${quote_mysql:${local_part:  $2}}'
and password='${quote_mysql:$3}'}{yes}{no}}
```

```
auth_login:
  driver                = plaintext
  public_name           = LOGIN
  server_set_id          = $1
  server_prompts         = Username:: : Password::
```

```
server_condition = ${lookup mysql{select login
from accounts where login='${quote_mysql:${local_part: $1}}'
and password='${quote_mysql:$2}'}{yes}{no}}
```

```
auth_cram_md5:
  driver = cram_md5
  public_name = CRAM-MD5
  server_secret = ${lookup mysql{select password
from accounts where login='${quote_mysql:
${local_part:$1}}'}{$value}fail}
  server_set_id = $1
```

5. Теперь настроим dovecot, редактируем

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

```
auth_default_realm = mail.nixtalk.com
auth_verbose = yes
base_dir = /var/run/dovecot/
disable_plaintext_auth = no
first_valid_gid = 8
first_valid_uid = 118
```

```
login_greeting = Dovecot ready
log_path = /var/log/dovecot.log
login_log_format_elements = user=<%u> method=%m rip=%r lip=%l
%c
```

```
mail_access_groups = mail
mail_debug = yes
mail_location = maildir:/home/mail/%d/%n
```

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

```
protocols = pop3 imap
service auth {
  unix_listener auth-master {
    mode = 0600
    user = Debian-exim
```

```

    }
    user = root
}
service imap-login {
    chroot = login
    inet_listener imap {
        address = *
        port = 143
    }
    process_limit = 3
    process_min_avail = 3
    service_count = 1
    user = dovecot
    vsz_limit = 64 M
}

service pop3-login {
    chroot = login
    inet_listener pop3 {
        address = *
        port = 110
    }
    process_limit = 3
    process_min_avail = 3
    service_count = 1
    user = dovecot
    vsz_limit = 64 M
}

ssl = no
#ssl_cert = </etc/ssl/certs/favmail.pem
#ssl_key = </etc/ssl/certs/favmail.pem

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

verbose_proctitle = yes
#protocol imap {
#    imap_client_workarounds = delay-newmail    tb-extra-mailbox-

```

```
sep  
#}
```

```
protocol pop3 {  
    pop3_client_workarounds = outlook-no-nuls oe-ns-eoh  
    pop3_uidl_format = %08Xu%08Xv  
}
```

```
protocol lda {  
    auth_socket_path = /var/run/dovecot/auth-master  
    postmaster_address = support@nixtalk.com  
}
```

6. Редактируем конфиг dovecot для доступа к mysql базе

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

```
driver=mysql  
connect=host=127.0.0.1      dbname=exim_db      user=exim  
password=eximPassword  
default_pass_scheme=PLAIN  
password_query=select password from accounts where login='%n'  
and domain='%d'  
user_query=select uid, gid from accounts where login='%n' and  
domain='%d'
```

7. Создаем директорию для писем и даем ей права

```
mkdir /home/mail  
chown Debian-exim:exim /home/mail
```

8. Прописываем в /etc/hosts IP нашего почтового сервера

```
77.124.5.76 nixtalk.com  
77.124.5.76 mail.nixtalk.com
```

На этом настройка закончена и в конце даю короткие команды где смотреть логи

```
tailf /var/log/dovecot.log  
tailf /var/log/exim4/mainlog  
tailf /var/log/exim4/rejectlog  
tailf /var/log/exim4/paniclog # Появляется при фатальных  
ошибках
```

Перезапуск сервисов

```
service dovecot restart  
service exim4 restart
```