

Postfix

Установка

```
apt install postfix postfix-ldap
```

Настройка

По умолчанию, Postfix пытается посылать почту в напрямую используя, запросы к [DNS](#), в частности записи типа MX.

relay_domains	список доменов, на которые разрешена пересылка писем
relayhost	имя и порт сервера для пересылки на него писем

Если имя заключено в квадратные скобки [] — то Postfix не предпринимает попытку поиска записей типа MX.

OpenLDAP

[OpenLDAP](#)

⚠ Схема Postfix не совместима с схемой [Misc](#)

[postfix.ldif](#)

[olcDbIndex_postfix.ldif](#)

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: mailRoutingAddress eq
```

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/postfix.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f olcDbIndex_postfix.ldif
```

[postfix.schema](#)

Псевдонимы

Для псевдонимов (Aliases) требуется инициализации БД (файл срасширением .db)

Файл	Команда
/etc/aliases	newaliases

⚠ Если возникает ошибка

```
postfix: warning: dict_nis_init: NIS domain name not set - NIS lookups disabled
```

Нужно установить переменную:

[/etc/postfix/main.cf](#)

```
alias_maps = hash:/etc/aliases
```

Маскарад адресов

Address masquerading

Замена одного домена или адреса другим, удобно использовать, если нужно скрыть внутренние домены при отправке почты на внешние адреса.

[/etc/postfix/main.cf](#)

```
smtp_generic_maps = hash:/etc/postfix/generic
```

[/etc/postfix/generic](#)

```
@foo.example.com          @example.com
```

Компиляция generic.db:

```
postmap /etc/postfix/generic
```

[Postfix Address Rewriting](#)

Размер сообщения

[/etc/postfix/main.cf](#)

```
message_size_limit = 30720000
```

Задается в Байтах, значение по умолчанию 10240000

Копирование всей почты

Отправка скрытых копий всех писем (Blind carbon copy) на определенный адрес.

[/etc/postfix/main.cf](#)

```
receive_override_options = no_address_mappings  
always_bcc = bcc@localhost.localdomain  
transport_maps = hash:/etc/postfix/transport  
receive_override_options =
```

В данном примере использован локальный адрес: bcc@localhost.localdomain

Команды

Проверка синтаксиса:

```
postfix -c ПУТЬ_К_ФАЙЛУ_НАСТРОЕК_main.cf check
```

Состояние очереди:

```
postqueue -c ПУТЬ_К_ФАЙЛУ_НАСТРОЕК_main.cf -p
```

Обработка очереди немедленно:

```
postqueue -c ПУТЬ_К_ФАЙЛУ_НАСТРОЕК_main.cf -f
```

Очистка очереди:

```
postsuper -c ПУТЬ_К_ФАЙЛУ_НАСТРОЕК_main.cf -d ALL
```

Тест адреса доставки:

```
postmap -q address@domain.ru ldap:/etc/postfix/ldap-users.cf
```

тот-же тест с использованием ldapsearch

```
ldapsearch -h 127.0.0.1 -p 389 -x -b "ou=users,dc=domain" -LLL '(&(!(l=disabled))(|(mail=info@domain.ru)(maildrop=info@domain.ru))(objectclass=mailUser))' maildrop
```

Работа с несколькими экземплярами



При решении некоторых задач можно воспользоваться возможностью работы с несколькими экземплярами (instance) сервера.

Для работы нужно добавить такие строки:

[/etc/postfix/main.cf](#)

```
multi_instance_enable = yes
multi_instance_wrapper = ${command_directory}/postmulti -p -g ИМЯ_ГРУППЫ reload
multi_instance_directories = /etc/postfix-mx /etc/postfix-l /etc/postfix-n
```

в переменной multi_instance_directories указывается экземпляры программы, в примере использованы следующие:

- /etc/postfix-mx
- /etc/postfix-l
- /etc/postfix-n

Для того, чтобы при запуске/останове и перезапуске Postfix и по команде

```
service postfix ...
```

нужно параметре multi_instance_wrapper нужно указать имя группы (ИМЯ_ГРУППЫ) в куда входя нужные экземпляры программы.

Также для того, чтобы разрешить работу с несколькими экземплярами можно использовать команду

```
postmulti -e init
```

Для управления служит программа postmulti.

Примеры:

Создание	<code>postmulti -I ИМЯ_ЭКЗЕМПЛЯРА -G ИМЯ_ГРУППЫ -e create</code>
Активация	<code>postmulti -i ИМЯ_ЭКЗЕМПЛЯРА -e enable</code>
Управление экземпляром	<code>postmulti -i ИМЯ_ЭКЗЕМПЛЯРА -p КОМАНДА</code>

Managing multiple Postfix instances on a single host

Удаление экземпляра

При удалении экземпляра нужно удалить его папку: `/var/spool/ИМЯ_ЭКЗЕМПЛЯРА`, иначе даже после того, как имя экземпляра удалено из переменной `multi_instance_directories` файла `/etc/postfix/main.cf` будет сообщение об ошибке:

`/var/log/mail.err`

```
postmulti[...]: fatal: No matching instances
```

Безопасность



<code>mynetworks</code>	список подсетей с которых разрешена отправка через этот сервер
<code>disable_vrfy_command = yes</code>	Клиент, подключившийся к серверу, может командой <code>vrfy user@domain.ru</code> определить, существует ли заданный адрес в системе
<code>show_user_unknown_table_name = no</code>	При попытке клиента отправить письмо несуществующему пользователю по умолчанию сервер выдаст 550 (reject) с сообщением <code>user unknown in local recipient table</code> (или другой таблице). Отключаем, пусть сервер сообщает <code>user unknown</code>
<code>smtpd_helo_required = yes</code>	Требуем от клиента приветствия (HELO/EHLO). Все, кто подключается, должны представляться
<code>smtpd_helo_restrictions=</code> <code> permit_mynetworks,</code> <code> permit_sasl_authenticated,</code> <code> reject_invalid_hostname,</code> <code> reject_non_fqdn_hostname,</code> <code> reject_invalid_helo_hostname,</code> <code> reject_unknown_helo_hostname</code>	Ограничения для этапа HELO/EHLO. Применяются к имени хоста, его IP-адресу и приветствию HELO/EHLO: Разрешаем доверенные сети Разрешаем тем, кто прошёл аутентификацию Отбрасываем неправильное (несуществующее) имя хоста Отбрасываем не полностью определённое доменное имя хоста Отбрасываем, если хост по HELO/EHLO не имеет A или MX записи
<code>smtpd_sender_restrictions=</code> <code> reject_non_fqdn_sender,</code> <code> reject_unknown_sender_domain,</code> <code> reject_unlisted_sender,</code> <code> permit_mynetworks,</code> <code> permit_sasl_authenticated</code>	Ограничения для этапа MAIL FROM. Применяется ко всему предыдущему + имя отправителя: Отбрасываем не полностью определённое имя отправителя Отбрасываем отправителя с несуществующего домена Отбрасываем несуществующих отправителей Проверяем отправителя. Если с нашего домена, то проверим, находится ли он в доверенной сети или прошёл аутентификацию Разрешаем отправлять с доверенных сетей Разрешаем отправлять прошедшим аутентификацию
<code>smtpd_recipient_restrictions=</code> <code> reject_non_fqdn_recipient,</code> <code> reject_unknown_recipient_domain,</code> <code> reject_unlisted_recipient,</code> <code> permit_mynetworks,</code> <code> permit_sasl_authenticated,</code> <code> reject_unauth_destination</code> <code> reject_invalid_hostname</code>	Ограничения для этапа RCPT TO. Применяется к предыдущему + имя получателя: reject, если получатель отсутствует в списке нашего домена или списке пересылки. Чтобы сервер не стал открытым relay

<pre>smtpd_data_restrictions= reject_unauth_pipelining, reject_multi_recipient_bounce</pre>	Ограничения для этапа DATA: Отвергаем запрос, когда клиент посылает команды SMTP раньше времени reject клиента с пустым именем отправителя, который отправляет сразу нескольким получателям
<pre>smtpd_etrn_restrictions= permit_mynetworks, permit_sasl_authenticated, reject</pre>	Ограничиваем клиентов, которые могут запрашивать очистку очереди сообщений

Пример

Пример для вставки в файл main.cf

```
disable_vrfy_command = yes
show_user_unknown_table_name = no
smtpd_helo_required = yes

smtpd_helo_restrictions=
  check_helo_access hash:/etc/postfix/helo_restrictions
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_invalid_hostname,
  reject_non_fqdn_hostname,
  reject_invalid_helo_hostname,
  reject_unknown_helo_hostname

smtpd_sender_restrictions=
  reject_non_fqdn_sender,
  reject_unknown_sender_domain,
  reject_unlisted_sender,
  permit_mynetworks,
  permit_sasl_authenticated

smtpd_recipient_restrictions=
  check_sender_access hash:/etc/postfix/sender_access
  reject_non_fqdn_recipient,
  reject_unknown_recipient_domain,
  reject_unlisted_recipient,
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_unauth_destination
  reject_invalid_hostname

smtpd_data_restrictions=
  reject_unauth_pipelining,
  reject_multi_recipient_bounce

smtpd_etrn_restrictions=
  permit_mynetworks,
  permit_sasl_authenticated,
  reject

message_size_limit = 51200000
```

Таблицы:

[/etc/postfix/helo_restrictions](#)

```
80.84.114.82    OK
mail.aqmh.ru    OK
```

```
aqmh.ru OK
aqmhdc.aqmh.com OK
mailpn.ru REJECT
stmails.ru REJECT
5.63.152.144 REJECT
```

[/etc/postfix/sender_access](#)

```
80.84.114.82 OK
mail.aqmh.ru OK
aqmh.ru OK
aqmhdc.aqmh.com OK
mailpn.ru REJECT
stmails.ru REJECT
5.63.152.144 REJECT
@mailpn.ru REJECT
```

Скрипт для компиляции таблиц:

[/etc/postfix/update_db.sh](#)

```
#!/bin/bash

postmap helo_restrictions sender_access transport
```

Интеграция с другими программами

AMaViSd-new

[AMaViSd-new](#) — интерфейс между MTA и сканером вирусов/фильтром содержания

[main.cf](#)

```
content_filter=smtp-amavis:[127.0.0.1]:10024
```

После транспорта pickup:

```
-o content_filter=
-o receive_override_options=no_header_body_checks
```

В конец файла:

```
smtp-amavis unix      -      -      n      -      2      smtp
-o smtp_data_done_timeout=1200
-o smtp_send_xforward_command=yes
-o smtp_tls_note_starttls_offer=no
127.0.0.1:10025 inet    n      -      n      -      -      smtpd
-o content_filter=
-o smtpd_delay_reject=no
-o smtpd_client_restrictions=permit_mynetworks,reject
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o smtpd_data_restrictions=reject_unauth_pipelining
```

```
-o smtpd_end_of_data_restrictions=
-o smtpd_restriction_classes=
-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 smtpd_client_connection_count_limit=0
-o smtpd_client_connection_rate_limit=0
-o receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters
-o local_header_rewrite_clients=
-o smtpd_milters=
-o local_recipient_maps=
-o relay_recipient_maps=
```

ClamAV

⚠ Для работы через [ClamSMTPd](#)

[main.cf](#)

```
content_filter = scan:127.0.0.1:10025
receive_override_options = no_address_mappings
```

[master.cf](#)

```
# AV scan filter (used by content_filter)
scan    unix  -      -      n      -      16      smtp
        -o smtp_send_xforward_command=yes
# For injecting mail back into postfix from the filter
127.0.0.1:10026 inet  n      -      n      -      16      smtpd
        -o content_filter=
        -o receive_override_options=no_unknown_recipient_checks,no_header_body_checks
        -o smtpd_helo_restrictions=
        -o smtpd_client_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o mynetworks_style=host
        -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

/etc/clamsmtpd.conf

```
OutAddress: 127.0.0.1:10026
```

Dovecot

[Dovecot](#)

[/etc/postfix/main.cf](#)

```
mailbox_command = /usr/lib/dovecot/dovecot-lda -f "$SENDER" -a "$RECIPIENT"
```

[/etc/postfix/master.cf](#)

```
dovecot    unix    -      n      n      -      -      pipe
        flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/dovecot-lda -f ${sender} -d
        ${recipient}
```

SpamAssassin

Эта настройка позволяет работать с [SpamAssassin](#) без использования [AMaViSd-new](#)

В файл `/etc/postfix/master.cf` нужно добавить

1. Для `smtp` и `submission` строку:

```
-o content_filter=spamassassin
```

пример:

```
...
smtp      inet  n       -       y       -       -       smtpd
          -o content_filter=spamassassin
...
submission inet n       -       y       -       -       smtpd
          -o content_filter=spamassassin
...
```

2. В конец файла:

```
spamassassin unix -      n      n      -      -      pipe
               user=debian-spamd argv=/usr/bin/spamc -f -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

3. Выполнить:

```
postfix reload
```

или

```
service postfix reload
```

SSL

Пример настройки работы по порту 587, с использованием сертификатов [Let's Encrypt](#):

[/etc/postfix/main.cf](#)

```
smtpd_tls_cert_file=/etc/letsencrypt/live/domain.ru/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/domain.ru/privkey.pem

smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_local_domain =
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_auth_enable = yes

smtp_tls_security_level = may
smtpd_tls_security_level = may
smtp_tls_note_starttls_offer = yes
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
```

Ссылки

- <https://wiki.debian.org/Postfix>
- ClamSMTP: Using with Postfix
- Postfix: документация postfix, ссылки, обмен опытом, форум :: Просмотр темы - Типовой конфиг для всех
- Postfix, warning: dict_nis_init.
- <https://wiki.debian.org/PostfixAndSASL>
- <http://wiki2.dovecot.org/HowTo/PostfixAndDovecotSASL>
- Postfix TLS Support
- **Очистка и обслуживание почтовой базы postfix**
- **Запрет писем с поддельным полем From или спам от себя к себе в postfix**
- Лимиты в Postfix. Ограничение на размер сообщения. Лимит на количество сообщений
- Настройка Postfix для отправки почты через внешний SMTP

<http://sysadminmosaic.ru/postfix/postfix>

2024-04-14 14:22

