Курс «Администратор Linux»

LAMP: Mail subsystem

Занятие # 28

Дмитрий Молчанов
Григорий Ожегов

Цель занятия

Обзор компонентов почтовой системы и базовых нюансов их конфигурирования.

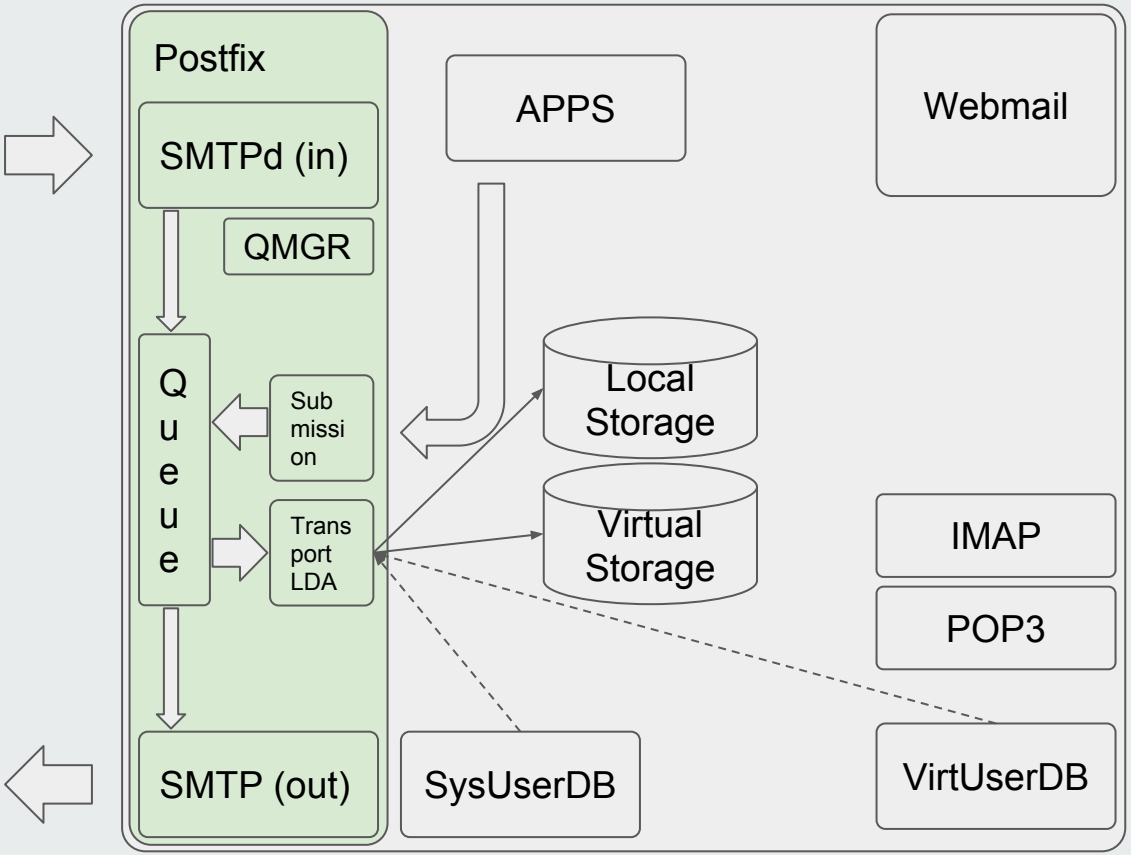
План

- обзор используемого ПО
- настройка отправки
  - хитрости
  - дополнения
- настройка приема
- хранение и доставка

Обзор используемого ПО

- MTA - postfix. Postfix пришел на смену популярному на заре интернет sendmail. Основными его плюсам является легкая и гибкая конфигурация, поддержка DNSBL, поддержка milter API.
- MDA - dovecot.
- Дополнительное ПО:
  - opendkim

Компоненты почтовой системы



Краткий обзор конфигурации postfix

- /etc/postfix - каталог с конфигурацией
  - main.cf - основной файл конфигурации, в котором хранится информация о настройках MTA. Проверить текущую конфигурацию и эффективные/умолчательные значения переменных можно с помощью команды `postconf`
  - master.cf - файл конфигурации master-процесса, который управляет остальными процессами postfix по требованию, своеобразный процесс-управляющий. В этом файле хранится конфигурация о том какие подпроцессы как запускать и как с ними взаимодействовать.
- map'ы - Часть конфигурации MTA хранится в map'ах - неких справочниках, куда MTA "подглядывает" по необходимости, например alias_maps/alias_database - справочник локальных псевдонимов для пользователей. ссылку на map легко опознать по формату: $format:$path (hash:/etc/aliases). Некоторые форматы справочников требуют компиляции с помощью команды `postmap $format:$path`.
  Поддерживаются различные форматы: **hash**,btree,**regex**,**cidr**,sqlite,mysql,ldap,tcp

Настройка отправки (smtp)

Наиболее частый пример использования почтовых сервисов - отправка почты от проекта.

Стоит разделить “отправку” на:

- отправку
- доставку

Для корректной отправки настроек необходимо немного и, в основном, это настройка не MTA, а “окружения” - ip/dns и приложения (использования корректных адресов). Также необходим доступ на tcp/25 наружу.

Настройка отправки (smtp)

- MTA
  - Адрес отправки (smtp_bind_address[6])
  - helo_hostname (smtp_helo_name)
- ip/DNS:
  - Важна “правильность” helo_hostname.
  - Важно наличие PTR-записи у ip с которого мы соединяемся ($inet_interfaces)
  - важно соответствие helo_hostname (A->) ip (PTR->) helo_hostname

```
[root@Net-R1 postfix]# telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 Net-R1.rt ESMTP Postfix  <- Server(smtpd) helo hostname (smtpd_banner=$myhostname ESMTP $mail_name)
HELO localhost               <- Client(smtp) helo hostname (smtp_helo_name=$myhostname)
250 Net-R1.rt
quit
221 2.0.0 Bye
```

Настройка отправки (smtp)

```
[root@Net-R1 postfix]# postconf | egrep '^smtp(_(helo_name|bind_address)|d_banner)'
smtp_bind_address =
smtp_bind_address6 =
smtp_helo_name = $myhostname
smtpd_banner = $myhostname ESMTP $mail_name
```

Полезные хитрости при отправке

- Помощь приложению с подстановкой правильного адреса:

```
sender_canonical_maps = hash:/etc/postfix/canonical
canonical:
 root@Net-R1.rt dmitry@molchanov.pp.ru
```

- Разные настройки smtp в зависимости от адреса отправителя:

```
main.cf:
 sender_dependent_default_transport_maps = hash:/etc/postfix/sender_based_transport
sender_based_transport:
 app@domain.tld   smtp-4app:
master.cf:
 smtp-4app  unix  -       -       -       -       -       smtp
        -o syslog_name=smtp-4app
        -o smtp_setting=value
```

- Разные настройки smtp в зависимости от домена назначения:

```
main.cf:
 transport_maps = regexp:/etc/postfix/transport
transport:
 /^@domain.tld$/  smtp-5c:
master.cf:
 smtp-5c   unix  -       -       -       -       -       smtp
       -o syslog_name=smtp-5c -o default_destination_concurrency_limit=5
       -o smtp_destination_concurrency_limit=5 -o smtp-5c_destination_concurrency_limit=5
```

Отправка: Очередь, отслеживание

Не смотря на то, что попытка отправки сообщения происходит незамедлительно, сообщение все равно попадает в очередь. При постановке сообщения в очередь ему присваивается идентификатор.

```
250 2.0.0 Ok: queued as 8E076195B61
```

По этому идентификатору сообщение можно отслеживать в логах:

```
grep 8E076195B61 /var/log/maillog
```

Или в очереди с помощью команд **mailq** или **postcat**. Также в логах мы можем увидеть сообщения с подстрокой вида

```
status=sent (250 OK id=1eyC63-00036j-DW)
```

Которая тоже сообщит нам id сообщения на удаленной стороне, что может быть полезно при общении с администратором этой системы в случае проблем

Отправка/Доставка: Дополнительно

Для повышения вероятности доставки сообщения сейчас рекомендуется использовать технологии направленные на борьбу со спамом:

- SPF (Sender Policy Framework) - Проверка описательной DNS-записи с каких адресов возможна отправка.
- DKIM (DomainKey Identified Mail) - Использование частных/публичных ключей для подписи/проверки сообщения, при этом частный ключ хранится на сервере, а публичный распространяется через DNS.

Обе технологии подразумевают добавление DNS-записей для домена. DKIM требует использования дополнительного ПО для подписи сообщений/проверки подписи, которые интегрируется с postfix через milter-api. Очень часто для этого используют OpenDKIM.

Прием почты

С приемом почты связано чуть больше настроек и здесь тоже не все настройки производятся на почтовом сервере:

- DNS - MX/A записи:
  - Домен должен обслуживаться как минимум 1 MX-сервером. В противном случае почта будет идти на сервер которому сопоставлена A (AAAA)-запись домен
  - В качестве mx-сервера должно быть использовано доменное имя имеющее A(не CNAME) запись.
  - helo_hostname не обязан принадлежать домену, который обслуживается данными сервером.
- Firewall - необходимо открыть 25 и 465 для доступа из вне сервера. 465й порт для smtp over ssl.
- MTA:
  - bind-адреса
  - обслуживаемые домены
  - способы доставки (локальный транспорт)
  - Ограничения доставки

Прием почты: MTA

- inet_interfaces - адреса на которых будут прослушиваться smtpd-сокеты (tcp/25, tcp/465)
- mydestination - домены обрабатываемые этим сервером
- relay_domains - домены для которых сервер принимает почту, чтобы потом передать далее. Могут использоваться справочники (map)
- ограничения доставки:
  - message_size_limit - ограничение принимаемого сообщения
  - mynetworks - список сетей которым сервер доверяет и принимает от них любую почту, от остальных будет приниматься только почта для mydestination и relay_domains
  - smtpd_*_restrictions - применение списков проверок.

Прием почты: ограничения

Ограничения служат в основном для борьбы с “бесполезной” почтой - спамом. Чтобы понять как и когда можно применять какие-либо ограничения можно посмотреть на процесс приема почты поподробнее:
Процесс приема почты можно разделить на несколько фаз:

1. Установление входящего соединения (получаем client_address)
    a. проверка локальных доступов по адресу
    b. проверка адреса в dnsbl
    c. проверка наличия обратной зоны
2. SMTP-handshake (получаем remote_helo_hostname)
3. Передача “конверной” информации (получаем sender и recipient)
4. Передача тела письма (получаем само письмо)

Задача фильтров - снизить поток нелегитимной почты которая доходит до content-фильтров/пользователя

Прием почты: ограничения

Ограничения служат в основном для борьбы с “бесполезной” почтой - спамом. Чтобы понять как и когда можно применять какие-либо ограничения можно посмотреть на процесс приема почты поподробнее:
Процесс приема почты можно разделить на несколько фаз:

1. Установление входящего соединения (получаем client_address)
2. SMTP-handshake (получаем remote_helo_hostname)
    a. проверка соответствия helo_hostname обратной зоне
3. Передача “конверной” информации (получаем sender и recipient)
4. Передача тела письма (получаем само письмо)

Задача фильтров - снизить поток нелегитимной почты которая доходит до content-фильтров/пользователя

Прием почты: ограничения

Ограничения служат в основном для борьбы с “бесполезной” почтой - спамом. Чтобы понять как и когда можно применять какие-либо ограничения можно посмотреть на процесс приема почты поподробнее:

Процесс приема почты можно разделить на несколько фаз:

1. Установление входящего соединения (получаем client_address)
2. SMTP-handshake (получаем remote_helo_hostname)
3. Передача “конверной” информации (получаем sender и recipient)
    a. проверка наличия отправителя
    b. проверка домена отправителя в dnsbl(rhsbl)
    c. проверка SPF отправителя
    d. проверка наличия получателя
4. Передача тела письма (получаем само письмо)

Задача фильтров - снизить поток нелегитимной почты которая доходит до content-фильтров/пользователя

Прием почты: ограничения

Ограничения служат в основном для борьбы с “бесполезной” почтой - спамом. Чтобы понять как и когда можно применять какие-либо ограничения можно посмотреть на процесс приема почты поподробнее:
Процесс приема почты можно разделить на несколько фаз:

1. Установление входящего соединения (получаем client_address)
2. SMTP-handshake (получаем remote_helo_hostname)
3. Передача “конверной” информации (получаем sender и recipient)
4. Передача тела письма (получаем само письмо)
    a. Проверка DKIM-подписей
    b. Контент-анализ

Задача фильтров - снизить поток нелегитимной почты которая доходит до content-фильтров/пользователя

Доставка и хранение.

Принимаемая почта может условно быть разделена на 3 разных категории:

- локальная системная - почта направленная системным пользователям.
- локальная виртуальная - аналог виртуальных хостов для почты - основываясь на домене получателя мы можем иметь разные непересекающиеся пространства имен email-адресов получателей, самое главное - отвязанных от системных пользователей. Для такой почты используются справочники virtual.
- проходящаяя почта (relay).

Доставка и хранение.

Почта адресованая локальным и виртуальным получателям и доставляемая средствами postfix (транспорт local, virtual) может храниться в 2х форматах:

- mailbox
- Maildir

Оба формата одинаково популярны и имеют свои преимущества/недостатки.

для включения доставки в формате Maildir на указать / в конце значения параметра mail_spool_directory для local-транспорта и в пути до mailbox’а для virtual-транпорта.

OpenDKIM

OpenDKIM используется для подписания/проверки DKIM-сигнатур. Настраивается в 2х местах - в DNS в поддомене _domainkeys создаются записи-для хранения публичных ключей селекторов которыми подписывается почта. На сервере запускается процесс который подключается через milter-api к MTA и занимается подписыванием определенных сообщений соответсвующими ключами-селекторами, что настраивается в конфигурации демона.

Спасибо за внимание

Дмитрий Молчанов
Григорий Ожегов