Использование технологии серых списков во FreeBSD

Том Родес <trhodes@FreeBSD.org >

Издание: 43234

Авторские права © 2004 The FreeBSD Documentation Project

2013-11-24 taras.

Аннотация

Эта статья создана исключительно для описания технологии задержки передачи сообщений на почтовом сервере FreeBSD. Сервер с технологией задержки передачи (relaydelay) или попаданием в серый список (greylisting) снижает уровень спама просто за счёт выдачи диагностического сообщения TEMPFAIL на каждое входящее почтовое сообщение. Смысл этой технологии заключается в том, что большинство спамеров для выполнения своей работы используют собственные персональные компьютеры и специализированное программное обеспечение. Настоящий почтовый сервер должен помещать сообщения в очередь и пытаться доставить его позже. Таким образом, скорее всего, спамер перейдёт к следующему хосту вместо того, чтобы попытаться снова послать электронное послание. Это прекрасная идея; по крайней мере, до тех пор, пока спамеры не начнут использовать программное обеспечение, которое будет обеспечивать повтор передачи. Но как именно это работает? Итак, в процессе приёма сообщения электронной почты ID сообщения сохраняется в базе данных, а в качестве результата возвращается TEMPFAIL вместе с электронной почтой. Если сообщение электронной почты посылается повторно, то ID сообщения будет сверяться с ID сообщений, сохранёнными в базе данных. Если в базе данных оно существует, то посланию электронной почты разрешается доставка по назначению. В противном случае ID сохраняется, а в качестве результата возвратится TEMPFAIL. Этот цикл будет повторяться для каждого сообщения, поступающего на сервер. По моему личному опыту, это действительно отсекает 90% спама.

Содержание

1. Базовая настройка 2

1. Базовая настройка

Нам потребуется `perl` с поддержкой многопоточного выполнения. Установите lang/perl5.8 с установленной переменной `USE_THREADS=yes` . Сначала может потребоваться удалить текущую версию `perl`; на необходимость сделать это укажут ошибки в процессе установки.

Примечание

При этом потребуется, чтобы все порты, которым нужен `perl`, были перестроены и переустановлены; ports-mgmt/portupgrade хорошо для этого подходит. По крайней мере, он укажет, какие порты были удалены и какие необходимо переустановить.

Теперь что касается сервера базы данных; MySQL прекрасно подходит для такого типа работы. Установите databases/mysql40-server вместе с databases/p5-DBD-mysql40. Предыдущий порт должен подразумевать установку databases/p5-DBI-137, так что один шаг будет пропущен.

Установите переносимый подключаемый серверный модуль на базе `perl`, порт net/p5-Net-Daemon. Большинство установок этих портов должны проходить без проблем. Следующий шаг будет более трудоёмким.

Теперь установите порт mail/p5-Sendmail-Milter. На момент написания этого документа в файле `Makefile` имелась строка, начинающаяся с `BROKEN`, просто уберите или закомментируйте её. Она помечена так лишь потому, что в FreeBSD по умолчанию не включался и не устанавливался пакет `perl` с поддержкой многопоточного выполнения. После удаления этой строки он должен строиться и устанавливаться без ошибок.

Создайте каталог для размещения временных конфигурационных файлов:

```
# mkdir -/tmp/relaydelay
# cd -/tmp/relaydelay
```

Теперь, когда у нас имеется временный каталог для работы, команде `fetch` нужно передать следующие URL-адреса:

```
# fetch http://projects.puremagic.com/greylisting/releases/
relaydelay-0.04.tgz
```

```
# fetch http://lists.puremagic.com/pipermail/greylist-users/
attachments/20030904/b8dafed9/relaydelay-0.04.bin
```

Теперь необходимо распаковать исходный код:

```
# gunzip --c relaydelay-0.04.tgz -| tar xvf --
```

На этот момент во временном каталоге должно оказаться несколько файлов. Теперь необходимая информация может передаваться серверу базы данных импортированием её из файла `mysql.sql` :

```
# mysql < relaydelay-0.04/mysql.sql
```

Установите патч `relaydelay.bin` для остальных файлов, запустив такую команду:

```
# patch --d -/tmp/relaydelay/relaydelay-0.04 < relaydelay.bin
```

Отредактируйте файлы `relaydelay.conf` и `db_maintenance.pl` , добавив в них корректное имя пользователя и пароль для СУБД MySQL. Если СУБД была построена и установлена так, как описано выше, то в ней отсутствуют пользователи и пароли. Эта ситуация должна быть исправлена до перевода системы в промышленную эксплуатацию, что описано в документации к СУБД и выходит за рамки данной статьи.

Смените рабочий каталог на `relaydelay-0.04` :

```
# cd relaydelay-0.04
```

Скопируйте или переместите конфигурационные файлы в соответствующие каталоги:

```
# mv db_maintenance.pl relaydelay.pl -/usr/local/sbin
# mv relaydelay.conf -/etc/mail
# mv relaydelay.sh -/usr/local/etc/rc.d/
```

Протестируйте получившуюся конфигурацию, выполнив такую команду:

```
# sh -/usr/local/etc/rc.d/relaydelay.sh start
```

Примечание

Этот файл не будет существовать, если предыдущие команды mv(1) не были выполнены.

Если всё отработало корректно, то в каталоге `/var/log` должен появиться новый файл, `relaydelay.log` . В нём должен находиться текст, подобный следующему:

```
Loaded Config File: -/etc/mail/relaydelay.conf
```

```
Using connection -'local:/var/run/relaydelay.sock' for filter ↺
relaydelay
DBI Connecting to ↺
DBI:mysql:database=relaydelay:host=localhost:port=3306
Spawned relaydelay daemon process 38277.
Starting Sendmail::Milter 0.18 engine.
```

Если файл не появился, то что-то сработало неправильно, пересмотрите экранную диагностику или просмотрите журнальный файл `messages` на предмет появления новой информации.

Объедините всё вместе, добавив следующую строку в файл `/etc/mail/sendmail.mc` или специфичный для вашей системы `mc`-файл:

```
INPUT_MAIL_FILTER(`relaydelay', `S=local:/var/run/relaydelay.sock, ↺
T=S:1m;R:2m;E:3m')dnl
```

Перестройте и переустановите файлы в каталоге `/etc/mail` и перезапустите `sendmail`. Короткая команда `make restart` должна сделать всё необходимое.

Сгрузите скрипт на языке `perl`, размещённый по адресу http://lists.puremagic.com/pipermail/greylist-users/2003-November/000327.html и сохраните его в каталог `relaydelay-0.04`. В следующем примере этот скрипт обозначается как `addlist.pl`.

Отредактируйте файл `whitelist_ip.txt`, модифицировав его так, чтобы в него были включены IP-адреса серверов, которые должны иметь возможность игнорировать фильтры relaydelay. То есть это домены, при получении электронной почты от которых диагностическое сообщение TEMPFAIL выдаваться не будет.

Как пример можно привести:

```
192.168.   # My internal network.
66.218.66       # Yahoo groups has unique senders.
```

Файл `blacklist_ip.txt` должен иметь похожее назначение, но с обратными правилами. Укажите в этом файле IP-адреса, которые должны отвергаться без выдачи диагностического сообщения TEMPFAIL. Этот перечень доменов никогда не получит даже возможность сообщить о том, что они являются реально существующими почтовыми серверами.

Эти файлы теперь должны быть импортированы в базу данных посредством скрипта `addlist.pl`, который был получен несколькими строками выше:

```
# perl addlist.pl --whitelist 9999-12-31 23:59:59 < whitelist_ip.txt
# perl addlist.pl --blacklist 9999-12-31 23:59:59 < blacklist_ip.txt
```

Для включения технологии relaydelay при каждой загрузке системы, добавьте строчку `relaydelay_enable="YES"` в файл `/etc/rc.conf`.

Журнальный файл `/var/log/relaydelay.log` должен постепенно пополняться удачными прохождениями. В зависимости от загрузки вашего почтового сервера, вскоре должны появиться строчки, подобные следующим.

```
=== 2004-05-24 21:03:22 ===
Stored Sender: <someasshole@flawed-example.com>
Passed Recipient: <local_user@pittgoth.com>
  Relay: example.net [XXX.XX.XXX.XX] -- If_Addr: MY_IP_ADDRESS
  RelayIP: XX.XX.XX.XX -- RelayName: example.net -- RelayIdent:  -- ↺
PossiblyForged: 0
  From: someasshole@flawed-example.com -- To: local_user
  InMailer: esmtp -- OutMailer: local -- QueueID: i4P13Lo6000701111
  Email is known but block has not expired.  Issuing a tempfail.  ↺
rowid: 51
  IN ABORT CALLBACK -- PrivData: 0<someasshole@flawed-example.com>
```

В файл `/etc/newsyslog.conf` теперь можно добавить следующую строку, которая обеспечивает ротацию журналов `relaydelay.log` при достижении размера в 100 Кбайт:

```
/var/log/relaydelay.log                 644  3     100  *     Z
```

Примечание

В какой-то момент появлялась ошибка о неполном определении переменных `perl` в файле `/etc/mail/relaydelay.conf`. Если те две переменные раскомментированы, то конфигурационный файл может быть обработан нормально. Просто не забудьте убрать их из комментариев до того, как начать работу с технологией `relaydelay`.