

Настройка fail2ban для защиты ssh соединения

Fail2ban — простой в использовании локальный сервис, который отслеживает log-файлы запущенных программ, и на основании различных условий блокирует по IP найденных нарушителей.

Программа умеет бороться с различными атаками на все популярные *NIX-сервисы, такие как Apache, Nginx, ProFTPD, vsftpd, Exim, Postfix, named, и т.д.

Но в первую очередь Fail2ban известен благодаря готовности «из коробки» к защите SSH-сервера от атак типа «bruteforce», то есть к защите SSH от перебора паролей.

Установка

Если до этого вы не обновляли базы данных apt, то установку можно начать с этого:

```
sudo apt update
sudo apt upgrade
```

После обновления apt можно переходить к установке Fail2ban:

```
sudo apt install fail2ban
```

Теперь активируем Fail2ban, чтобы она автоматически запускалась после перезагрузки сервера:

```
sudo systemctl enable fail2ban
```

Перед запуском Fail2ban в работу осталось настроить параметры фильтрации, по которым будет происходить блокировка IP.

Настройка

По умолчанию Fail2ban использует правила блокировки, указанные в файле *jail.conf*. Это системный файл, который обновляется вместе с программой, поэтому использовать его в качестве основного файла с параметрами блокировки не рекомендуется.

Мы создадим собственный конфигурационный файл *jail.local*. Система приоритетов в Fail2ban настроена таким образом, что в качестве основных применяются правила, указанные в *jail.local*.

Структура конфигурационного файла

Конфигурационный файл Fail2ban состоит из так называемых jail-ов — отдельных блоков правил для разных служб. В одном файле *jail.local* можно не только указать все правила для всех сетевых служб сервера, но и управлять их включением и выключением.

Структура всех jail-ов одинакова:

1. В первой строке в квадратных скобках указывают название службы, к которой будет применяться следующий ниже набор правил. В нашем случае это **[sshd]**.
2. Далее определяют параметр **enabled**, отвечающий за включение или отключение данного jail-а. Мы установим его **true**, чтобы наш jail был активен.
3. После этого указывают условия блокировки: максимальное количество попыток подключения (**maxretry**), время, за которое эти попытки были произведены (**findtime**), и время, на которое нужно запретить доступ с этого IP (**bantime**).
4. В последней части jail-а указывают IP-адреса, которые считаются надёжными (**ignoreip**), например, IP-адрес вашего домашнего компьютера.

Мы рекомендуем добавить в строку **ignoreip** домашний адрес вашего компьютера, чтобы в случае особо жёстких настроек фильтрации программа не заблокировала вам доступ к серверу — например, после нескольких неудачных попыток ввода пароля.

Создадим конфигурационный файл:

```
sudo vim /etc/fail2ban/jail.local
```

Текст конфигурационного файла будет примерно таким:

```
[sshd]
enabled  = true
maxretry = 6
findtime = 1h
bantime  = 1d
ignoreip = 127.0.0.1/8 22.33.44.55
```

Этот набор условий означает, что IP-адрес, с которого было произведено 6 неудачных попыток SSH-подключения за последний час (3600 секунд), будет заблокирован на одни сутки (86400 секунд). Не будут блокироваться IP-адреса локальной машины и адрес 22.33.44.55.

Время для параметров **findtime** и **bantime** можно указывать не только в секундах, но и в минутах, часах, днях и даже неделях. Для этого необходимо сразу после численного значения параметра указать соответствующую букву (m, h, d, w).

Начало работы

После создания конфигурационного файла, содержащего все необходимые правила, можно запускать Fail2ban и наблюдать за его работой.

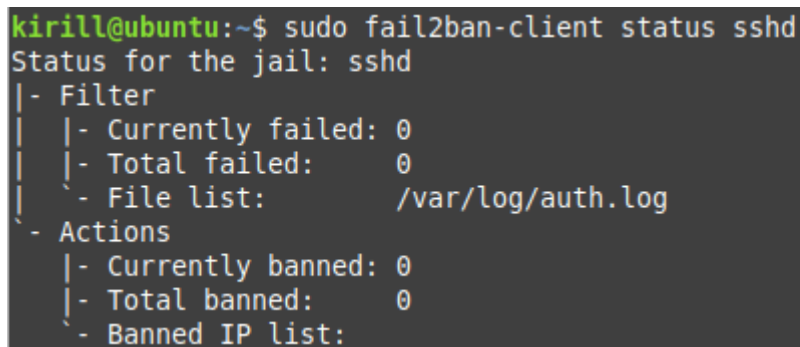
Команда для запуска программы:

```
sudo systemctl start fail2ban
```

Команда для вывода на экран сведений о работе jail-а, отвечающего за службу **sshd**:

```
sudo fail2ban-client status sshd
```

Если в данный момент сервер не подвергается атаке, сразу после установки и запуска программы на экране будет следующая информация:



```
kirill@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:    0
|   `-- File list:      /var/log/auth.log
`- Actions
    |- Currently banned: 0
    |- Total banned:    0
    `-- Banned IP list:
```

Здесь приведены сведения о попытках подключения к серверу и о заблокированных IP-адресах.

Если вы решите изменить настройки, указанные в конфигурационном файле *jail.local*, не забудьте перезапустить Fail2ban, чтобы изменения вступили в силу:

```
sudo systemctl restart fail2ban
```

Как удалить из fail2ban заблокированный ip

Сперва проверьте iptables командой:

```
sudo iptables -S
```

Вот что мы увидели в консоли:

```
kirill@ubuntu:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-N f2b-sshd
-A INPUT -p tcp -m multiport --dports 22 -j f2b-sshd
-A f2b-sshd -s 85.93.129.152/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -j RETURN
```

IP адрес 85.93.129.152 заблокирован сервисом fail2ban.

Выводим список всех наших клеток (jail) следующей командой:

```
sudo fail2ban-client status
```

```
kirill@ubuntu:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:  sshd
```

Здесь может быть много правил для служб, но в нашем примере указан только sshd.

Вывод списка IP для конкретной клетки (для конкретного jail):

```
sudo fail2ban-client status sshd
```

```
kirill@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    6
| `-- File list:      /var/log/auth.log
`- Actions
  |- Currently banned: 1
  |- Total banned:    1
  `-- Banned IP list:  85.93.129.152
```

Для того чтобы разбанить (удалить ИП с заблокированного листа) необходимо выполнить следующую команду:

```
sudo fail2ban-client set sshd unbanip ip-адрес
```

```
kirill@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:    6
|   \- File list:      /var/log/auth.log
\-- Actions
    |- Currently banned: 1
    |- Total banned:    1
    \- Banned IP list:  85.93.129.152
kirill@ubuntu:~$ sudo fail2ban-client set sshd unbanip 85.93.129.152
1
kirill@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:    6
|   \- File list:      /var/log/auth.log
\-- Actions
    |- Currently banned: 0
    |- Total banned:    1
    \- Banned IP list:
```

Если Вы не хотите, чтобы данный ip адрес снова был заблокирован, то добавьте его в файл jail.local в секцию [sshd] в строчку ignoreip.

Версия #4

Кирилл создал 8 февраля 2024 15:02:12

Кирилл обновил 8 февраля 2024 15:45:22