Установка и настройка fail2ban (0.9.6)

- Установка службы
- Конфигурация службы
- Блокировка по умолчанию
- Параметры блокировок и их изменение
- Использование преднастроенных фильтров
- Создание своих фильтров и сценариев
- Выключение ошибочной блокировки

Служба `fail2ban` ограничивает возможность подбора паролей и поиска уязвимостей сетевых сервисов, блокируя доступ к этим сервисам для узлов, производящих подозрительные действия. Такая возможность может быть очень полезна для сетевых сервисов, доступ к которым необходим из сети Интернет.

Данная статья применима к:

- ОС ОН Орёл 2.12

Установка службы

Установить службу **fail2ban** можно с помощью графического менеджера пакетов или из командной строки командой:

```
sudo apt install fail2ban
```

Конфигурация службы

Служба fail2ban работает с четырьмя типами конфигурационных файлов:

Файл(ы)	Описание
/etc/fail2ban/fail2ban.conf /etc/fail2ban/fail2ban.local	Глобальные настройки службы и настройки "по умолчанию"
/etc/fail2ban/filter.d/*.conf /etc/fail2ban/filter.d/*.local	Фильтры, определяющие действия для обнаружения неудачных попыток аутентификации. В общем случае, это правила анализа системных журналов.
/etc/fail2ban/action.d/*.conf /etc/fail2ban/action.d/*.local /etc/fail2ban/action.d/*.py	Действия, определяющие порядок блокировки/разблокировки. В том числе, действия могут быть заданы как сценарии на языке Python (*.py).
/etc/fail2ban/jail.conf /etc/fail2ban/jail.local /etc/fail2ban/jail.d/*.conf /etc/fail2ban/jail.d/*.local	Определения комбинаций фильтров и действий.Фильтры и действия идентифицируются по именам файлов без расширений .conf/.local.

При этом конфигурационные файлы *.conf устанавливаются самой службой, и могут быть переписаны при обновлениях, а файлы *.local предназначены для постоянного хранения локальных изменений конфигурации, и обрабатываются после файлов *.conf, т.е. переопределяют значения, заданные в файлах *.conf.

Блокировка по умолчанию

По умолчанию служба fail2ban защищает сервер sshd. Эта блокировка включена в созданном при установке пакета файле /etc/fail2ban/jail.d/defaults-debian.conf.
Содержимое этого файла "по умолчанию":

```
[sshd]
enabled = true
```

При этом доступ блокируется на 10 минут, если неправильный пароль был введен 5 раз в течение 10 минут, а эти параметры блокировки заданы в файле /etc/fail2ban/jail.conf.

Параметры блокировок и их изменение

Блокировка определяется тремя параметрами:

Параметр	Описание
maxretry	Количество неудачных попыток
findtime	Период времени, в который запоминаются неудачные попытки
bantime	Период времени, на который блокируется доступ если за findtime случилось больше maxretry неудачных попыток

Параметры блокировок, принятые по умолчанию, указаны в файле /etc/fail2ban/jail.conf. Для изменения параметров их можно исправить в этом файле (не рекомендуется, так как файл может быть переписан при обновлении), либо (лучше) создать в каталоге /etc/fail2ban/jail.d/ файл с расширением .local и любым удобным именем, в котором переопределить значения параметров, например, файл/etc/fail2ban/jail.d/00-orel.local:

```
[DEFAULT]
bantime = 300
maxretry = 10
findtime = 3600
ignoreip = 10.0.15.0/24
```

В приведенном примере переопределяются следующие значения параметров:

- секция [DEFAULT] означает, что параметры будут применяться ко всем блокировкам по умолчанию;
- блокировка производится на 5 минут (300 секунд);
- дается 10 попыток ввода пароля;
- учитываются неудачные попытки входа в течение часа (3600 секунд);
- игнорируются попытки перебора пароля из сети 10.0.15.0/24.

После изменения конфигурации fail2ban нужно перезапустить, например, командой

```
sudo systemctl restart fail2ban
```

Использование преднастроенных фильтров

В составе fail2ban имеется ряд преднастроеных фильтров, определённых в файлах, содержащихся в каталоге /etc/fail2ban/filters.d/ (например, блокировка для защиты службы dovecot определена в /etc/fail2ban/filters.d/dovecot.conf).
Эти блокировки можно включать и использовать по мере необходимости. Для добавления других блокировок, кроме ssh, нужно создать в директории /etc /fail2ban/jail.d файл с расширением .local, содержащий переопределение секции соответствующего фильтра с параметром enabled=true.

Например, для защиты службы dovecot создадим файл /etc/fail2ban/jail.d/dovecot.local:

```
[dovecot]
enabled = true
bantime = 120
```

Имя применяемого фильтра определяется именем секции. В секции [dovecot] этого файла могут быть указаны специальные параметры (в примере - параметр bantime), которые будут применяться только для dovecot, переопределяя значения по умолчанию (в примере определено время блокировки как 2 минуты (120 секунд)). При этом может быть переопределён и применяемый фильтр (параметр filter).

Создание своих фильтров и сценариев

Свои фильтры и сценарии можно создавать в каталогах /etc/fail2ban/filter.d/ и /etc/fail2ban/action.d/, используя в качестве образцов предустановленные файлы, и сохраняя свои сценарии в файлах с расширением .local.

Выключение ошибочной блокировки

Если доступ оказался заблокирован по ошибке, его можно разблокировать командой:

```
fail2ban-client set < > unbanip <IP- >
```

Например, разблокировать доступ к ssh для узла 10.0.15.35 можно командой:

```
fail2ban-client set sshd unbanip 10.0.15.35
```

Более подробная информация по работе и настройке службы содержится в справочной системе man:

man fail2ban
man fail2ban-server
man fail2ban-client
man jail.conf