**Инструкция по установке**

**ПО “BOTBLOCK”**

**Содержание**

[Установка и настройка 3](#_heading=h.3znysh7)

[1. Системные требования 3](#_heading=h.2et92p0)

[2. Установка и конфигурация Nginx 3](#_heading=h.tyjcwt)

[3. Создание службы запуска модуля 4](#_heading=h.3dy6vkm)

[4. Конфигурация ПО 4](#_heading=h.1t3h5sf)

[5. Логи блокировки запроса 6](#_heading=h.4d34og8)

[Информация для контактов 6](#_heading=h.hf6fyok3mo3h)

# Установка и настройка

## 1. Системные требования

| **ОС** | Debian 11/12 |
| --- | --- |
| **Системный софт** | GCC 10 или выше |

## 2. Установка и конфигурация Nginx

Установить веб-сервер Nginx на отдельном сервере. В конфигурационный файл Nginx в блок http добавить следующие строки:

log\_format json\_combined escape=json

'{'

 '"timestamp":"$time\_iso8601",'

 '"host":"$host",'

 '"scheme":"$scheme",'

 '"port":"$server\_port",'

 '"node":"$hostname",'

 '"remote\_addr":"$remote\_addr",'

 '"remote\_user":"$remote\_user",'

 '"request":"$request\_uri",'

 '"status": "$status",'

 '"method": "$request\_method",'

 '"body\_bytes\_sent":"$body\_bytes\_sent",'

 '"http\_referrer":"$http\_referer",'

 '"http\_user\_agent":"$http\_user\_agent",'

 '"request\_time":"$request\_time",'

 '"uaddr":"$upstream\_addr",'

 '"uhost":"$proxy\_host",'

 '"uct":"$upstream\_connect\_time",'

 '"uht":"$upstream\_header\_time",'

 '"urt":"$upstream\_response\_time",'

 '"content\_type":"$sent\_http\_content\_type",'

 '"request\_id":"$request\_id"'

 '}';

 access\_log syslog:**server=ip:514**,facility=local7,tag=nginx,severity=info json\_combined;

В директиве access\_log syslog в параметре server указать IP-адрес сервера, где будет установлен Модуль анализа логов, и порт 514.

Логи будут сохраняться в директории /home/debian/crpt\_access\_logs на сервере, указанном в access\_log syslog:server.

## 3. Создание службы запуска модуля

На сервере, на котором будет работать ПО “BOTBLOCK”, создать файл /etc/systemd/system/**botcheck.service** (служба для запуска Модуля анализа логов)и добавить в него следующие строки:

 **[Unit]**

 Description=Bot checker

 After=network.target

 **[Service]**

 User=debian

 Group=debian

 ExecStart=<путь до файла crptab\_api> --conf /home/debian/crpt /config.ini

 Restart=on-failure

 WorkingDirectory=/home/debian

 AmbientCapabilities=CAP\_NET\_BIND\_SERVICE

 **[Install]**

 WantedBy=multi-user.target

где:

User=debian – пользователь, от которого будет запущен сервис с правами на чтение и запись,

Group=debian – группа с правами на чтение и запись,

параметр /home/debian/crpt/config.ini – конфигурационный файл модуля.

## 4. Конфигурация ПО

В конфигурационном файле ПО “BOTBLOCK” /home/debian/crpt/**config.ini** следует указать путь к файлам **rules.json, limits.json**:

 **[DEFAULT]**

 log\_level = ERROR

 log\_folder = /home/debian/app\_logs

 workers\_count = 4

 **[LogSaver]**

 path = /home/debian/crpt\_access\_logs

 buffer\_size = 33000000

 **[Rules]**

 rules\_file = **rules.json**

 default\_windows\_size = 1200

 default\_temporary\_ban\_time = 30

 temporary\_ban\_threshold = 2

 permanent\_ban\_threshold = 5

 default\_shift\_window = 1

 **[Limits]**

 limits\_file = **limits.json**

 default\_ban\_time = 10

 **[HttpServer]**

 listen\_address = 0.0.0.0

 listen\_port = 8080

 temporary\_ban\_path = /temporary.txt

 **[Syslog]**

 listen\_address = 0.0.0.0

 listen\_port = 514

где:

log\_level – уровень логирования; параметр может принимать значения: ERROR, WARNING, INFO; значение по умолчанию ERROR; в логах указывается тип сообщения, например, предупреждение: «LOG(warning) << “All ips has been unbaned”»; типы сообщений:

ERROR – сообщение об ошибке,

WARNING – предупреждение,

INFO – информационное сообщение;

log\_folder – файл логов приложения (с указанием абсолютного пути);

workers\_count – количество потоков > 1;

path – абсолютный путь до папки с логами;

buffer\_size – размер буфера с логами, при достижении которого логи сохраняются на диск; параметр задается в байтах; значение по умолчанию 67 108 864 байт = 64 × 1024 × 1024 байт;

rules\_file – файл с описанием Правил (с указанием абсолютного пути);

default\_windows\_size – время окна учета срабатываний Правил в секундах;

default\_temporary\_ban\_time – время временной блокировки по умолчанию в секундах;

temporary\_ban\_threshold – количество срабатываний для временной блокировки по умолчанию;

permanent\_ban\_threshold – количество срабатываний для постоянной блокировки по умолчанию; постоянной считается блокировка на 30 суток;

limits\_file – файл с описанием лимитов (с указанием абсолютного пути);

default\_ban\_time – время блокировки в секундах в случае нарушения одного из указанных лимитов;

default\_shift\_window – выполнять ли сдвиг окна после очередного срабатывания правил (1 – true, 0 – false);

listen\_address – адрес, на котором будет выполняться прием данных Syslog;

listen\_port – порт, на котором будет выполняться прием данных Syslog;

listen\_address – адрес, на котором будет выполняться прием HTTP-запросов;

listen\_port – порт, на котором будет выполняться прием HTTP-запросов;

temporary\_ban\_path – URI, на котором будет осуществляться прием запросов на текущий список заблокированных адресов;

## 5. Логи блокировки запроса

Логи модуля, которые помогут определить причину блокировки запроса, можно найти в папке /home/debian/app\_logs.

# Информация для контактов

Для контактов с командой разработчиков просьба обращаться по следующим контактам:

E-mail: support@weblock.ru