

## HTTP протокол

Практика выполняется на monitoring сервере, доступ к нему осуществляется по IP адресу и выполняются с root привилегиями.

Данная проверка предназначена для проверки сервисов с использованием HTTP протокола.

1. Добавляем в конфигурационный файл проверку по HTTP протоколу с именем проверки http\_slurm:

```
cat <<EOF >> /etc/blackbox_exporter/blackbox.yml
http_slurm:
  prober: http
  timeout: 2s
  http:
    preferred_ip_protocol: ip4
    valid_http_versions: ["HTTP/1.1", "HTTP/2"]
    valid_status_codes: [200]
    fail_if_not_ssl: true
    method: GET
    fail_if_body_not_matches_regexp:
      - "Prometheus"
```

EOF

В данной конфигурации для проверки используется протокол ip v4, проверяется версия HTTP, код ответа, метод GET. Также проверка закончится с ошибкой, если не используется https или если в ответе отсутствует слово: Prometheus.

2. Чтобы применить изменения, перезапускаем Blackbox Exporter:

```
systemctl restart blackbox_exporter
```

3. Проверка.

```
curl -is "http://localhost:9115/probe?module=http_slurm&target=http://prometheus.io" |
grep probe_success
```

В запросе, в качестве параметра module, передаётся имя проверки, а в качестве параметра target – адрес веб сайта, который проверяется. С помощью грег фильтруем результат, чтобы получить только результат проверки.

**NB!** Адрес сайта может передаваться вместе со схемой. Если схема не указана, то будет использоваться http.

Результат должен быть таким:

```
# HELP probe_success Displays whether or not the probe was a success
# TYPE probe_success gauge
probe_success 1
```

4. Полный список параметров для проверки по HTTP протоколу:

### **timeout**

Default: scrape\_timeout

Время, после которого проверка будет считаться неудачной. **NB!** Если значение не задано, используется scrape\_timeout, который передал Prometheus.

### **preferred\_ip\_protocol**

Default: ip6

Какой протокол используется для проверки. Допустимые значения: ip4| ip6.

### **source\_ip\_address**

Default: -

Если на сервере несколько IP адресов, можно указать, с какого ip будет проводиться проверка.

### **valid\_status\_codes**

default: 200

Проверка считается неудачной, если код не соответствует заданному.

### **valid\_http\_versions**

Проверка считается неудачной, если версия HTTP не соответствует строке.

### **method**

Default: GET

Тип запроса. Возможные значения: GET | POST.

## **headers**

Список заголовков, которые передаются во время проверки.

## **no\_follow\_redirects**

Default: false

Следовать ли редиректам при проверке.

## **fail\_if\_ssl**

Default: false

Проверка считается неуспешной, если соединение установлено по https.

## **fail\_if\_body\_matches\_regexp**

Проверка считается неуспешной, если в body присутствует строка удовлетворяющая регулярному выражению.

## **fail\_if\_body\_not\_matches\_regexp**

Проверка считается неуспешной, если в body отсутствует строка удовлетворяющая регулярному выражению.

## **fail\_if\_header\_matches**

Проверка считается неуспешной, если в ответе присутствует заголовок, значение которого удовлетворяет регулярному выражению.

- header – имя заголовка, который проверяется.
- regexp – регулярное выражение, которое проверяется в значении заголовка.
- allow\_missing – разрешить отсутствие заголовка. По умолчанию: false.

## **fail\_if\_header\_not\_matches**

Проверка считается неуспешной, если в ответе отсутствует заголовок, значение которого удовлетворяет регулярному выражению.

- **header** – имя заголовка, который проверяется.
- **regex** – регулярное выражение, которое проверяется в значении заголовка.
- **allow\_missing** – разрешить отсутствие заголовка. По умолчанию: `false`.

### **basic\_auth**

- **username** – имя пользователя, которое используется для авторизации на проверяемом сайте.
- **password** – пароль, который используется для авторизации на проверяемом сайте.

### **bearer\_token**

Токен для bearer авторизации.

### **bearer\_token\_file**

Файл, который содержит токен для bearer авторизации.

### **proxy\_url**

Адрес прокси сервера, если проверку необходимо выполнить через прокси сервер.

### **body**

Body, которое передается вместе с запросом.

### **tls\_config**

- **insecure\_skip\_verify** – проверять ли валидность сертификата. Значение по умолчанию: `false`
- **ca\_file** – путь к файлу с корневыми сертификатами.
- **cert\_file** – путь к файлу с клиентским сертификатом.
- **key\_file** – путь к файлу с клиентским ключом.
- **server\_name** – строка для проверки имени сервера.

