DNS протокол

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

Данная проверка предназначена для тестирования DNS серверов и наличия на них определенных записей.

1. Добавляем в конфигурационный файл проверку dns с именем dns_slurm:

```
cat <<EOF >> /etc/blackbox_exporter/blackbox.yml
  dns_slurm:
    prober: dns
    timeout: 2s
    dns:
      query_name: slurm.io
      preferred_ip_protocol: ip4
EOF
```

В данной конфигурации будет проверяться, может ли DNS сервер разрешить имя slurm.io.

2. Чтобы применить изменения, перезапускаем Blackbox Exporter:

systemctl restart blackbox_exporter

3. Проверяем работу:

curl -is "http://localhost:9115/probe?module=dns_slurm&target=8.8.8.8" | grep probe_success

В запросе, в качестве параметра module, передаётся имя проверки, а в качестве параметра target – на какой DNS сервер будет отправлен запрос. С помощью grep фильтруем результат, чтобы получить только результат проверки.

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 dns 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.

transport_protocol

Default: udp

Протокол, по которому будет производиться проверка. Возможные значения: udp, tcp.

query_name:

Default: -

Запрос, который будет отправлен на DNS сервер.

query_type

Default: "ANY"

Тип записи, который будет запрашиваться. По умолчанию, запрашиваются все типы записей.