ДЗ-08: Vector

Заменил logstash/filebeat на vector из конфигурации 6/7-го ДЗ: vector отправляет SSHD логи в elastic.

Установка

https://vector.dev/docs/setup/installation/

Конфиг

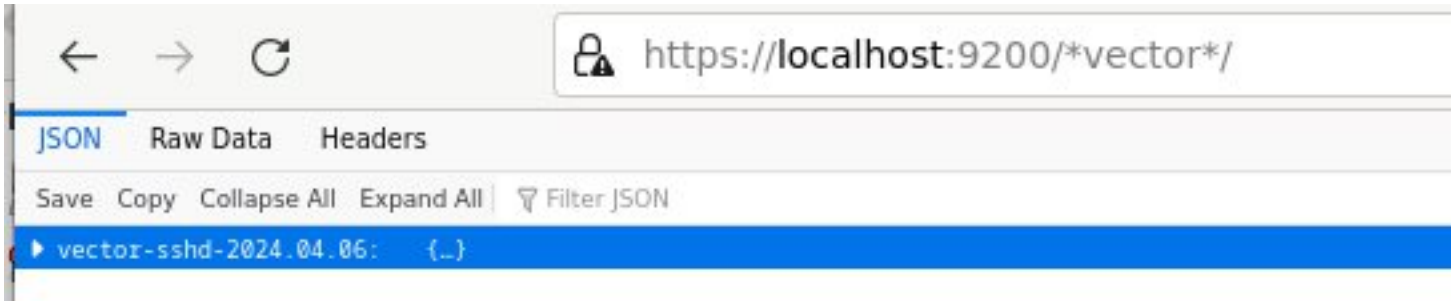
/etc/vector/vector.yaml

```
sources:
 sshd_http_source:
   type: "socket"
   address: "127.0.0.1:10514"
   mode: "udp"
   decoding:
     codec: "json"
 sshd_log_source:
   type: "file"
   read_from: "beginning"
   include:
     - "/var/log/sshd.log"


transforms:
  sshd_http_transform:
    type: "remap"
    inputs: ["sshd_http_source"]
    source: '.programname=upcase!(.programname) + "-from-vector-http"'
  sshd_log_transform:
    type: "remap"
    inputs: ["sshd_log_source"]
    source: |
     . |= parse_syslog!(.message)
     .@timestamp = .timestamp
     .programname = "SSHD-from-vector-log-file"

sinks:
  print:
    type: "console"
    inputs: ["sshd_http_transform", "sshd_log_transform"]
    encoding:
      codec: "json"
  es:
    type: "elasticsearch"
    inputs: ["sshd_*_transform"]
    endpoints: ["https://10.0.2.15:9200", "https://localhost:9200"]
    bulk:
      index: "vector-sshd-%Y.%m.%d"
    tls:
      verify_certificate: false
    auth:
      strategy: "basic"
      user: "elastic"
      password: "10DM27XoI52iiDxXZa78"
```

Индекс



Kibana