

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

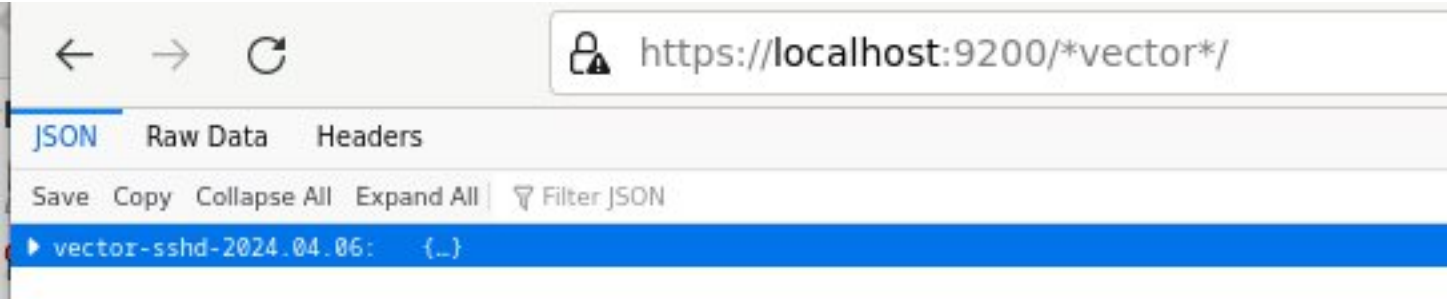
/etc/vector/vector.yaml

```
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: "10DM27Xol52iiDxXZa78"
```

Индекс



Kibana

elastic

Find apps, content, and more.

🔍

Discover

New Open Share Alerts Inspect Save

vector-sshd

Filter your data using KQL syntax

Selected fields

3

programname

message

timestamp

Popular fields

1

timestamp

Available fields

9

appname

file

host

hostname

message

procid

programname

source_type

timestamp

Unmapped fields

10

Add a field

74 hits

Documents

Field statistics

Get the best look at your search results

Take the tour

Dismiss

@timestamp

programname

2024-04-06T10:19:36.672Z

SSHD-from-vector-http

2024-04-06T10:19:33.392Z

SSHD-from-vector-http

2024-04-06T10:19:25.643Z

SSHD-from-vector-log-file

2024-04-06T10:19:25.642Z

SSHD-from-vector-log-file

2024-04-06T10:19:24.695Z

SSHD-from-vector-log-file

Rows per page: 100

Expanded document

View: Single document

K < 4 of 74 > |

Actions	Field	Value
	_id	iLLRso4BjqEIVEYhsHx7
	_index	vector-sshd-2024.04.06
	_score	-
	@timestamp	2024-04-06T10:19:33.392Z
	@version	1
	@version.keyword	1
	facility	auth
	facility.keyword	auth
	host	127.0.0.1
	message	Failed password for user from 127.0.0.1 port 46242 ssh2
	port	59824
	procid	19,371
	programname	SSHD-from-vector-http
	severity	info
	severity.keyword	info