# 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

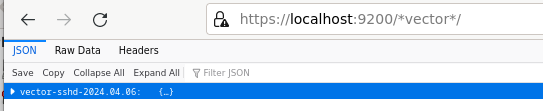
auth:

strategy: "basic"

user: "elastic"

password: "10DM27XoI52iiDxXZa78"

### Индекс



Kibana

