ДЗ-07: ELK-beats

Установка

https://www.elastic.co/guide/en/beats/heartbeat/current/heartbeat-installation-configuration.html
https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-installation-configuration.html
https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-installation-configuration.html

Конфиги

/etc/heartbeat/heartbeat.yml

```
heartbeat.monitors:
- type: http
  enabled: true
  id: otus-hw-monitor
  name: Otus HW Monitor
  urls: ["https://otus.ru", "https://google.com"]
  schedule: '@every 10s'


output.elasticsearch:
  hosts: ["localhost:9200"]
  preset: balanced
  protocol: "https"
  username: "elastic"
  password: "10DM27XoI52iiDxXZa78"
  ssl.verification_mode: none
```

/etc/metricbeat/metricbeat.yml

```
output.elasticsearch:
  hosts: ["localhost:9200"]
  preset: balanced
  protocol: "https"
  username: "elastic"
  password: "10DM27XoI52iiDxXZa78"
  ssl.verification_mode: none
```

Подключаем модуль

```
metricbeat modules enable system
```

/etc/metricbeat/modules.d/system.yml

```
- module: system
  period: 10s
  metricsets:
    - cpu
    - memory
  process.include_top_n:
    by_cpu: 5      # include top 5 processes by CPU
    by_memory: 5   # include top 5 processes by memory
```

/etc/filebeat/metricbeat.yml

```
output.elasticsearch:
  hosts: ["localhost:9200"]
  preset: balanced
  protocol: "https"
  username: "elastic"
  password: "10DM27XoI52iiDxXZa78"
  ssl.verification_mode: none
```

Подключаем модуль

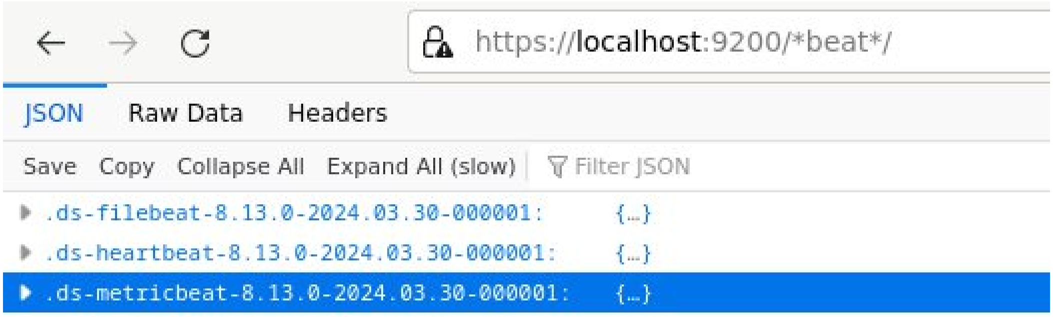
```
filebeat modules enable system
```

/etc/filebeat/modules.d/system.yml

```
- module: system
  syslog:
```

```
  enabled: true
auth:
  enabled: true
```

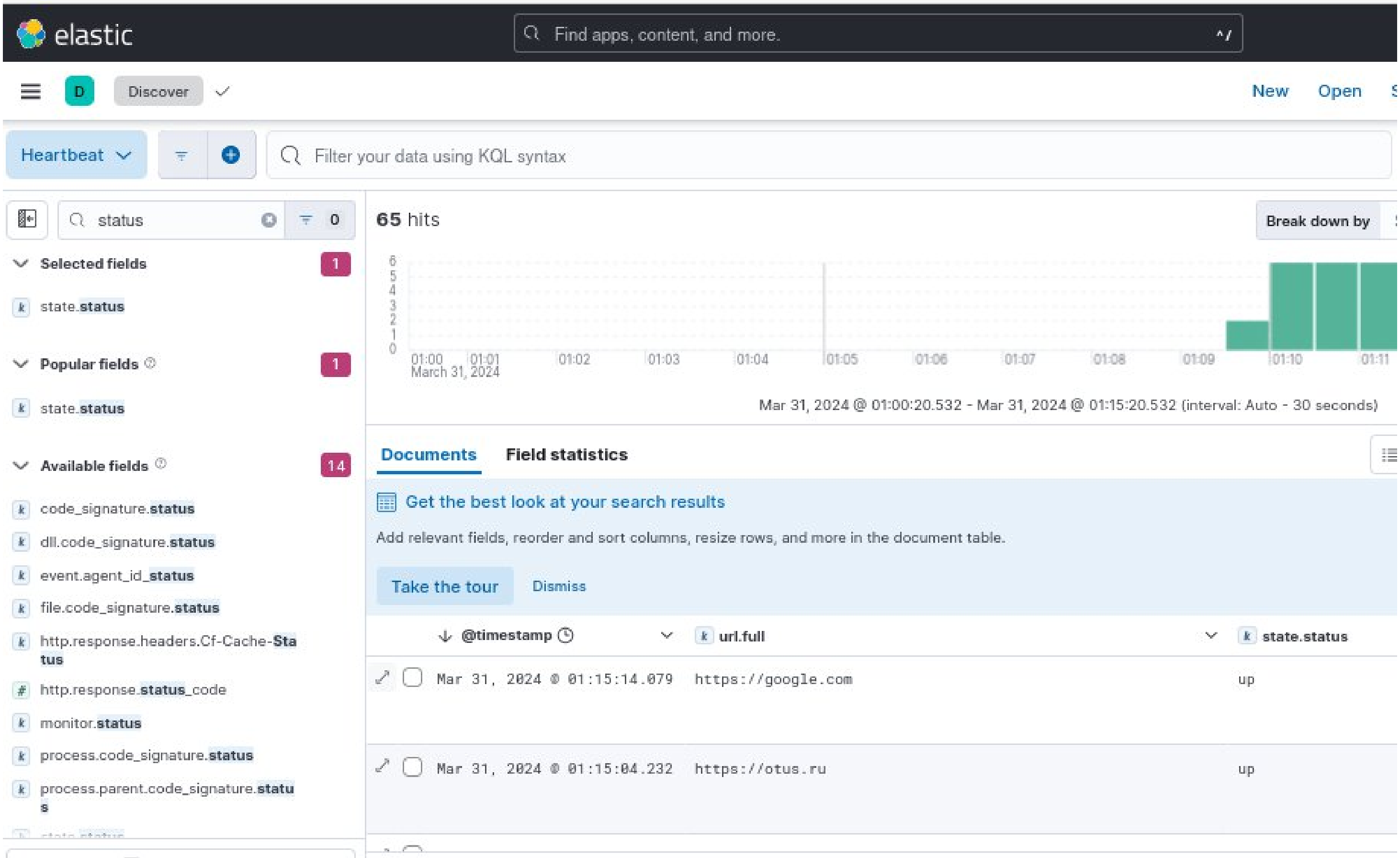
Индексы



https://localhost:9200/*beat*/

```
.ds-filebeat-8.13.0-2024.03.30-000001:      {…}
.ds-heartbeat-8.13.0-2024.03.30-000001:     {…}
.ds-metricbeat-8.13.0-2024.03.30-000001:    {…}
```

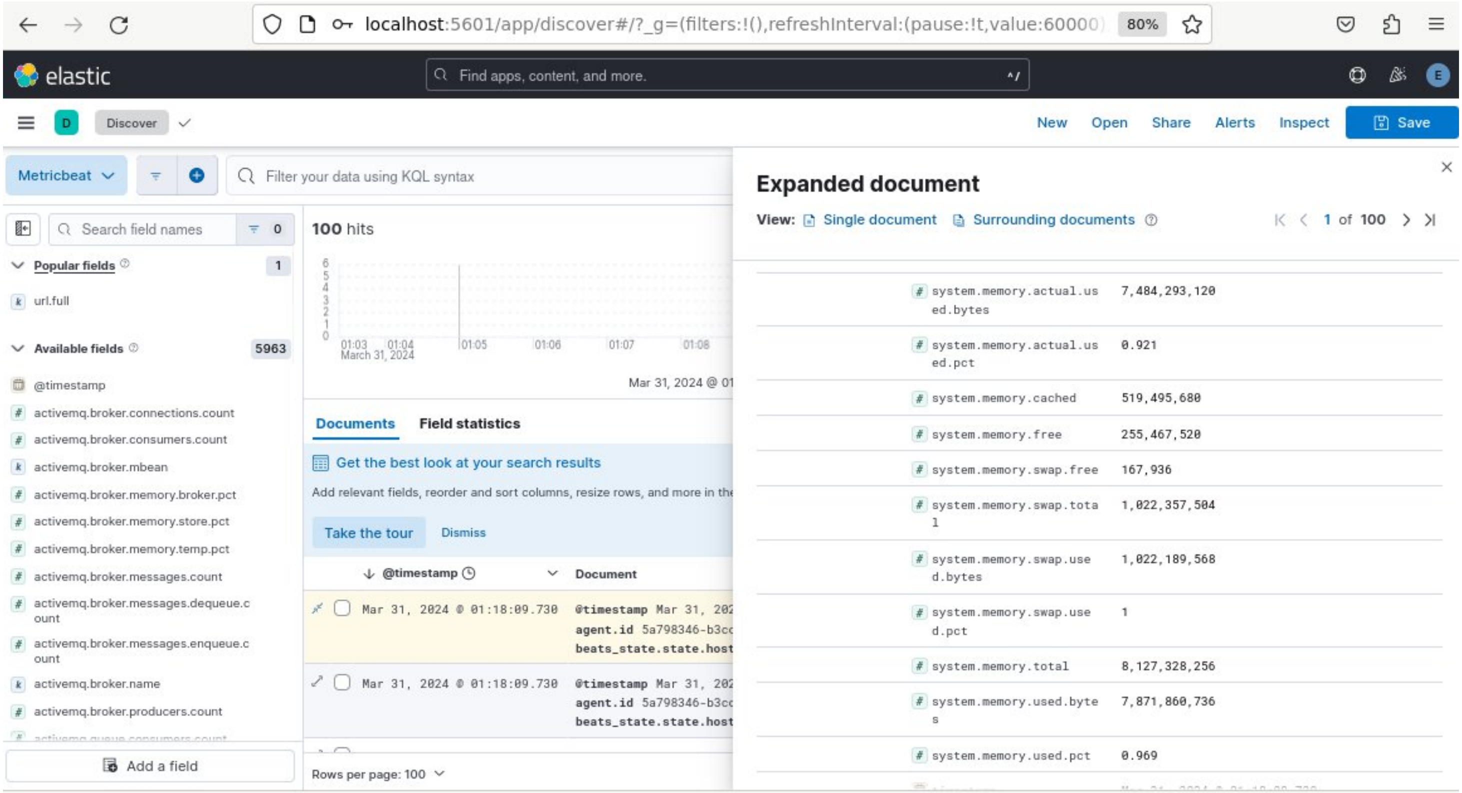
Kibana



elastic
Find apps, content, and more.
D
Discover
New
Open
Heartbeat
Filter your data using KQL syntax
status
0
Selected fields
1
state.status
Popular fields
1
state.status
Available fields
14
code_signature.status
dll.code_signature.status
event.agent_id_status
file.code_signature.status
http.response.headers.Cf-Cache-Status
http.response.status_code
monitor.status
process.code_signature.status
process.parent.code_signature.status
65 hits
Break down by
6
5
4
3
2
1
0
01:00
March 31, 2024
01:01
01:02
01:03
01:04
01:05
01:06
01:07
01:08
01:09
01:10
01:11
Documents
Field statistics
Get the best look at your search results
Add relevant fields, reorder and sort columns, resize rows, and more in the document table.
Take the tour
Dismiss

Mar 31, 2024 @ 01:00:20.532 - Mar 31, 2024 @ 01:15:20.532 (interval: Auto - 30 seconds)

@timestamp	url.full	state.status
Mar 31, 2024 @ 01:15:14.079	https://google.com	up
Mar 31, 2024 @ 01:15:04.232	https://otus.ru	up



Popular fields

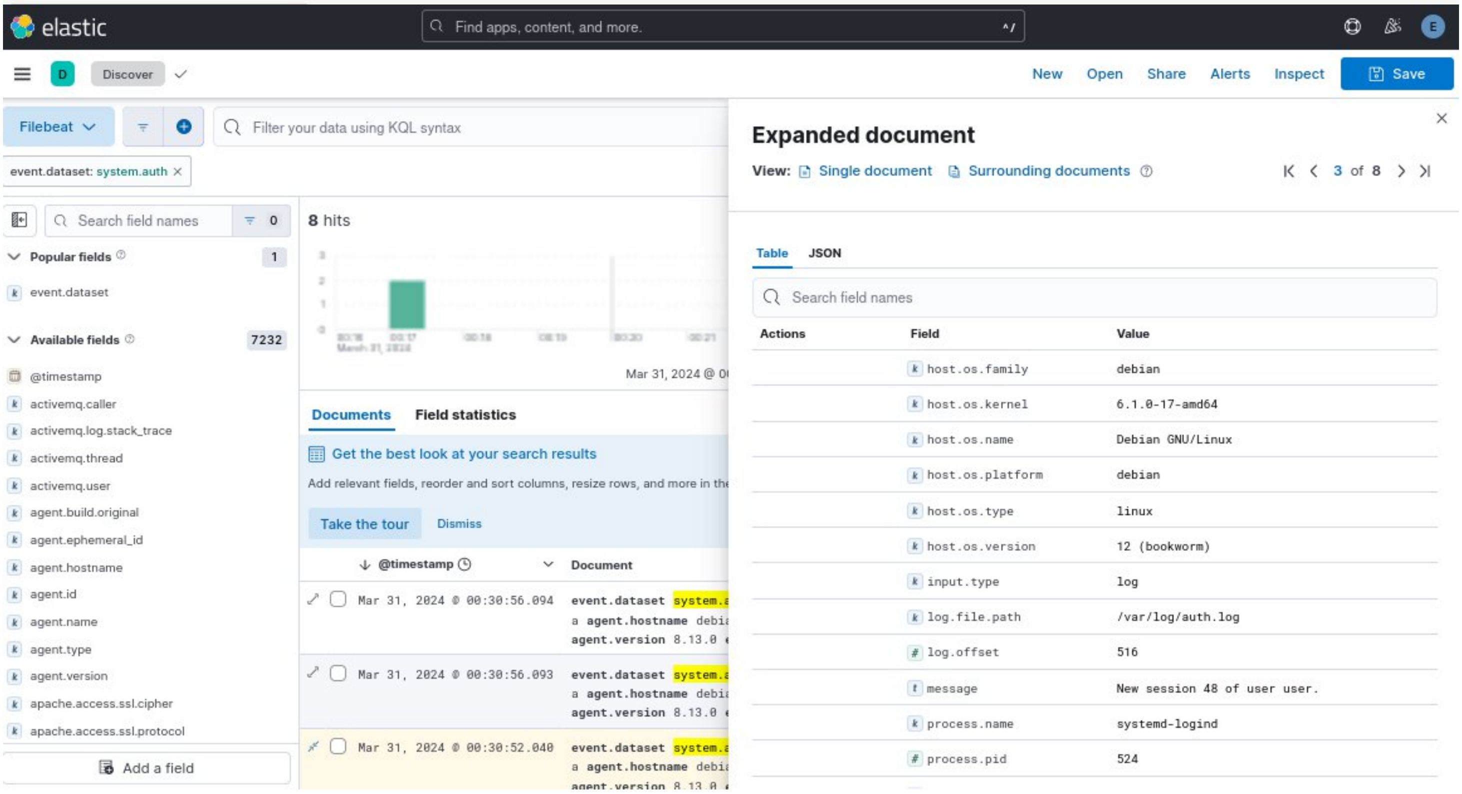
- url.full

Available fields

- @timestamp
- activemq.broker.connections.count
- activemq.broker.consumers.count
- activemq.broker.mbean
- activemq.broker.memory.broker.pct
- activemq.broker.memory.store.pct
- activemq.broker.memory.temp.pct
- activemq.broker.messages.count
- activemq.broker.messages.dequeue.count
- activemq.broker.messages.enqueue.count
- activemq.broker.name
- activemq.broker.producers.count

@timestamp	Document
Mar 31, 2024 @ 01:18:09.730	@timestamp Mar 31, 202 agent.id 5a798346-b3cc beats_state.state.host
Mar 31, 2024 @ 01:18:09.730	@timestamp Mar 31, 202 agent.id 5a798346-b3cc beats_state.state.host

Field	Value
system.memory.actual.used.bytes	7,484,293,120
system.memory.actual.used.pct	0.921
system.memory.cached	519,495,680
system.memory.free	255,467,520
system.memory.swap.free	167,936
system.memory.swap.total	1,022,357,504
system.memory.swap.used.bytes	1,022,189,568
system.memory.swap.used.pct	1
system.memory.total	8,127,328,256
system.memory.used.bytes	7,871,860,736
system.memory.used.pct	0.969



Popular fields

- event.dataset

Available fields

- @timestamp
- activemq.caller
- activemq.log.stack_trace
- activemq.thread
- activemq.user
- agent.build.original
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.name
- agent.type
- agent.version
- apache.access.ssl.cipher
- apache.access.ssl.protocol

@timestamp	Document
Mar 31, 2024 @ 00:30:56.094	event.dataset system.a a agent.hostname debi agent.version 8.13.0
Mar 31, 2024 @ 00:30:56.093	event.dataset system.a a agent.hostname debi agent.version 8.13.0
Mar 31, 2024 @ 00:30:52.040	event.dataset system.a a agent.hostname debi agent.version 8.13.0

Actions	Field	Value
	host.os.family	debian
	host.os.kernel	6.1.0-17-amd64
	host.os.name	Debian GNU/Linux
	host.os.platform	debian
	host.os.type	linux
	host.os.version	12 (bookworm)
	input.type	log
	log.file.path	/var/log/auth.log
	log.offset	516
	message	New session 48 of user user.
	process.name	systemd-logind
	process.pid	524