JSON   Raw Data   Headers

Save   Copy

```
name:                                    "node-1"
cluster_name:                            "my-application"
cluster_uuid:                            "asv2EAtOQv2qGmy1IY05EA"
▼ version:
    number:                              "7.2.0"
    build_flavor:                        "default"
    build_type:                          "rpm"
    build_hash:                          "508c38a"
    build_date:                          "2019-06-20T15:54:18.811730Z"
    build_snapshot:                      false
    lucene_version:                      "8.0.0"
    minimum_wire_compatibility_version:  "6.8.0"
    minimum_index_compatibility_version: "6.0.0-beta1"
    tagline:                             "You Know, for Search"
```

elasticsearch

Elasticsearch   ● Health is green   Basic license

Overview

| Version | 7.2.0 |
| Uptime | an hour |

Nodes: 1

Disk Available	81.90%
	13.9 GB / 17.0 GB
JVM Heap	11.62%
	117.1 MB / 1,007.4 MB

Indices: 4

Documents	17
Disk Usage	138.0 KB
Primary Shards	4
Replica Shards	0

Kibana   ● Health is green

Overview

| Requests | 10 |
| Max. Response Time | 260 ms |

Instances: 1

Connections	0
Memory Usage	21.03%
	306.2 MB / 1.4 GB

```
[2019-07-08T16:50:17,155][INFO ][logstash.javapipeline    ] Pipeline started {"pipeline.id"=>"main"}
[2019-07-08T16:50:17,220][INFO ][logstash.agent           ] Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
[2019-07-08T16:50:17,344][INFO ][filewatch.observingtail  ] START, creating Discoverer, Watch with file and sincedb collections
[2019-07-08T16:50:17,734][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:port=>9600}
```

```
HELLO, its test cheks for logstash
{
        "message" => "HELLO, its test cheks for logstash",
     "@timestamp" => 2019-07-08T14:53:57.153Z,
           "host" => "ELK1",
        "@version" => "1"
}
```

192.168.0.52:9200/_cat/shards

```
.kibana_task_manager          0 p STARTED     2   45.6kb 192.168.0.52 ELK2
.monitoring-es-7-2019.07.08   0 p STARTED  5278    3.3mb 192.168.0.52 ELK2
filebeat-7.2.0-2019.07.08-000001 0 p STARTED  100   33.5kb 192.168.0.52 ELK2
filebeat-7.2.0-2019.07.08-000001 0 r UNASSIGNED
.monitoring-kibana-7-2019.07.08 0 p STARTED  617  176.5kb 192.168.0.52 ELK2
.ogstash-2019.07.08-000001    0 p STARTED     0     283b 192.168.0.52 ELK2
.ogstash-2019.07.08-000001    0 r UNASSIGNED
.kibana_1                     0 p STARTED     5   73.9kb 192.168.0.52 ELK2
```

Elasticsearch

- Index Management
- Index Lifecycle Policies
- Rollup Jobs
- Cross-Cluster Replication
- Remote Clusters
- Snapshot Repositories
- License Management
- 8.0 Upgrade Assistant

Kibana

- Index Patterns
- Saved Objects
- Spaces
- Reporting
- Advanced Settings

Index Management

Update your Elasticsearch indices individually or in bulk.

○ ✕ Include rollup indices   ○ ✕ Include system indices

🔍 Search

Lifecycle status ⌄   Lifecycle phase ⌄   ↻ Reload indices

Name	Health	Status	Primaries	Replicas	Docs count	Storage size
logstash-2019.07.08-000001	● yellow	open	1	1	0	283b

Rows per page: 10 ⌄

192.168.0.51
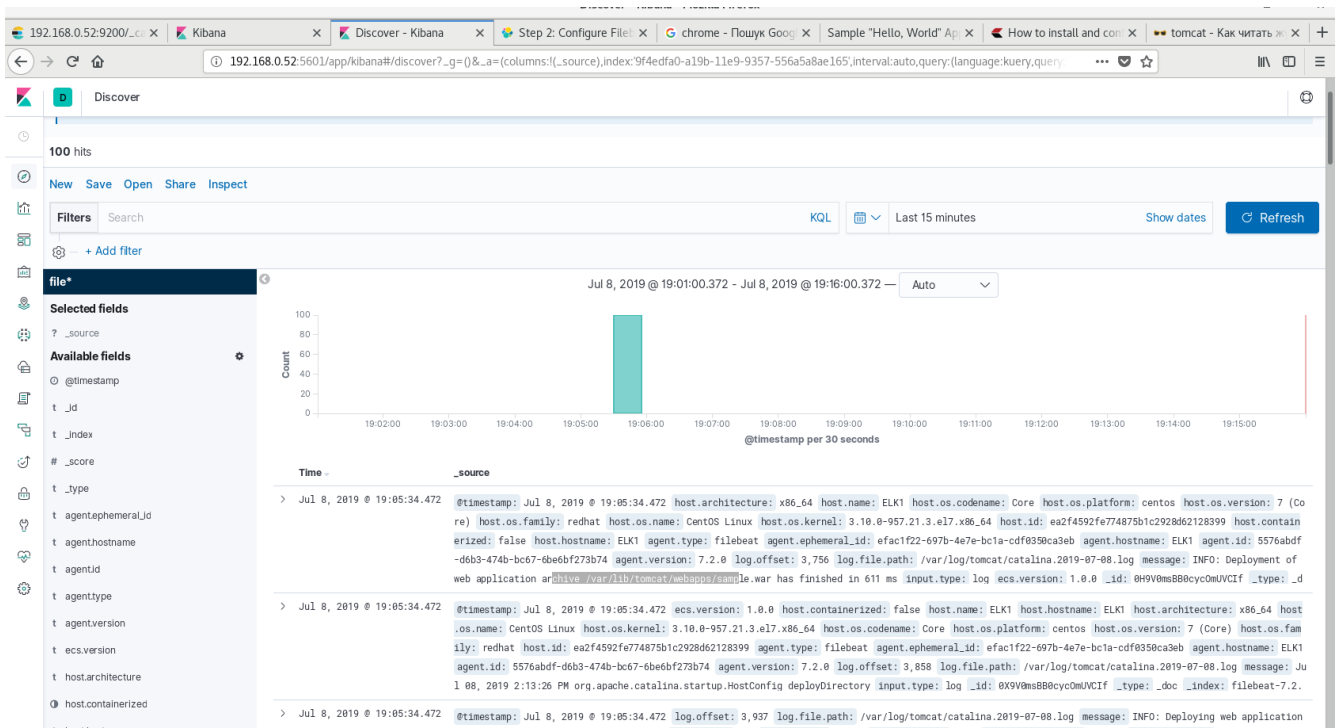
Sample "Hello, World" Applica

This is the home page for a sample application used to illustrate th Guide.

To prove that they work, you can execute either of the following links:

- To a JSP page.
- To a servlet.

192.168.0.52:5601/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:'9f4edfa0-a19b-11e9-9357-556a5a8ae165',interval:auto,query:(language:kuery,query

Discover

100 hits

New Save Open Share Inspect

Filters Search   KQL | 📅 ▾ Last 15 minutes   Show dates   🔄 Refresh

⚙ + Add filter

file*

Selected fields

? _source

Available fields ⚙

@timestamp

t _id

t _index

_score

t _type

t agent.ephemeral_id

t agent.hostname

t agent.id

t agent.type

t agent.version

t ecs.version

t host.architecture

◉ host.containerized

t host.hostname

Jul 8, 2019 @ 19:01:00.372 - Jul 8, 2019 @ 19:16:00.372 — Auto ▾

Count: 100, 80, 60, 40, 20, 0

19:02:00 19:03:00 19:04:00 19:05:00 19:06:00 19:07:00 19:08:00 19:09:00 19:10:00 19:11:00 19:12:00 19:13:00 19:14:00 19:15:00

@timestamp per 30 seconds

Time   _source

> Jul 8, 2019 @ 19:05:34.472 @timestamp: Jul 8, 2019 @ 19:05:34.472 host.architecture: x86_64 host.name: ELK1 host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.os.family: redhat host.os.name: CentOS Linux host.os.kernel: 3.10.0-957.21.3.el7.x86_64 host.id: ea2f4592fe774875b1c2928d62128399 host.containerized: false host.hostname: ELK1 agent.type: filebeat agent.ephemeral_id: efac1f22-697b-4e7e-bc1a-cdf0350ca3eb agent.hostname: ELK1 agent.id: 5576abdf-d6b3-474b-bc67-6be6bf273b74 agent.version: 7.2.0 log.offset: 3,756 log.file.path: /var/log/tomcat/catalina.2019-07-08.log message: INFO: Deployment of web application archive /var/lib/tomcat/webapps/sample.war has finished in 611 ms input.type: log ecs.version: 1.0.0 _id: 0H9V0msBB0cycOmUVCIf _type: _d

> Jul 8, 2019 @ 19:05:34.472 @timestamp: Jul 8, 2019 @ 19:05:34.472 ecs.version: 1.0.0 host.containerized: false host.name: ELK1 host.hostname: ELK1 host.architecture: x86_64 host.os.name: CentOS Linux host.os.kernel: 3.10.0-957.21.3.el7.x86_64 host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.os.family: redhat host.id: ea2f4592fe774875b1c2928d62128399 agent.type: filebeat agent.ephemeral_id: efac1f22-697b-4e7e-bc1a-cdf0350ca3eb agent.hostname: ELK1 agent.id: 5576abdf-d6b3-474b-bc67-6be6bf273b74 agent.version: 7.2.0 log.offset: 3,858 log.file.path: /var/log/tomcat/catalina.2019-07-08.log message: Jul 08, 2019 2:13:26 PM org.apache.catalina.startup.HostConfig deployDirectory input.type: log _id: 0X9V0msBB0cycOmUVCIf _type: _doc _index: filebeat-7.2.

> Jul 8, 2019 @ 19:05:34.472 @timestamp: Jul 8, 2019 @ 19:05:34.472 log.offset: 3,937 log.file.path: /var/log/tomcat/catalina.2019-07-08.log message: INFO: Deploying web application

---

Management / Index management

ⓘ Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. Read more

[Yes] [No]

🔶 **Elasticsearch**

Index Management
Index Lifecycle Policies
Rollup Jobs
Cross-Cluster Replication
Remote Clusters
Snapshot Repositories
License Management
8.0 Upgrade Assistant

🔷 **Kibana**

Index Patterns
Saved Objects
Spaces
Reporting
Advanced Settings

Index Management

Update your Elasticsearch indices individually or in bulk.

◯✕ Include rollup indices   ◯✕ Include system indices

🔍 Search   Lifecycle status ▾ Lifecycle phase ▾   🔄 Reload indices

☐	Name	Health	Status	Primaries	Replicas	Docs count	Storage size
☐	filebeat-7.2.0-2019.07.08-000001	🟡 yellow	open	1	1	100	33.5kb
☐	logstash-2019.07.08-000001	🟡 yellow	open	1	1	0	283b

Rows per page: 10 ▾

192.168.0.52:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2019-07-08T16:05:34.460Z',to:'2019-07-08T16:05:34.480Z'))&...

Discover

ⓘ Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. Read more

[Yes] [No]

1 hit

New Save Open Share Inspect

Filters 1 Search   KQL | 📅 ▾ Jul 8, 2019 @ 19:05:34.46 → Jul 8, 2019 @ 19:05:34.48   🔄 Refresh

⚙ message: Deployment of web application archive ✕ + Add filter

file*

Selected fields

? _source

Available fields ⚙

@timestamp

t _id

t _index

_score

t _type

t agent.ephemeral_id

t agent.hostname

t agent.id

t agent.type

t agent.version

Jul 8, 2019 @ 19:05:34.460 - Jul 8, 2019 @ 19:05:34.480 — Auto ▾

Count: 1, 0.8, 0.6, 0.4, 0.2, 0

19:05:34.462 19:05:34.464 19:05:34.466 19:05:34.468 19:05:34.470 19:05:34.472 19:05:34.474 19:05:34.476 19:05:34.478

@timestamp per millisecond

Time   _source

> Jul 8, 2019 @ 19:05:34.472 message: INFO: Deployment of web application archive /var/lib/tomcat/webapps/sample.war has finished in 611 ms @timestamp: Jul 8, 2019 @ 19:05:34.472 host.architecture: x86_64 host.name: ELK1 host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.os.family: redhat host.os.name: CentOS Linux host.os.kernel: 3.10.0-957.21.3.el7.x86_64 host.id: ea2f4592fe774875b1c2928d62128399 host.containerized: false host.hostname: ELK1 agent.type: filebeat agent.ephemeral_id: efac1f22-697b-4e7e-bc1a-cdf0350ca3eb agent.hostname: ELK1 agent.id: 5576abdf-d6b3-474b-bc67-6be6bf273b74 agent.version: 7.2.0 log.offset: 3,756 log.file.path: /var/log/tomcat/catalina.2019-07-08.log input.type: log ecs.version: 1.0.0 _id: 0H9V0msBB0cycOmUVCIf _type: _d

Kibana - Mozilla Firefox

192.168.0.52:9200/_cat/s ×   Kibana ×   Step 2: Configure Filebea ×   chrome - Пошук Google ×   Sample "Hello, World" Applic ×   How to install and config ×   tomcat - Как читать журн ×

192.168.0.52:5601/app/kibana#/visualize/create?type=pie&indexPattern=c4c1e690-a19d-11e9-9357-556a5a8ae165&_g=(filters:!())&_a=(filters:!(),linked:!f,query:(la

Visualize / Create

Save   Share   Inspect   Refresh

Filters   Search   KQL   Off   Refresh

+ Add filter

fil*

Data   Options

Metrics

> Slice Size Count

Buckets

∨ Split Slices

Aggregation   Filters help

Filters

Filter 1

Deployment

Filter 2

Undeployment

⊕ Add filter

> Advanced

Add sub-buckets

● Deployment
● Undeployment

field   value
level 1 Deployment 3 (100%)

war   ∧ ∨   Highlight All   Match Case   Whole Words   1 of 2 matches   Reached end of page, continued from top

mc [root@E...   Kibana - Mo...   Skype [1]   Oracle VM V...   ELK2 [Runni...   Kibana - Go...   Project — ~...   [student : b...   Double Co...   Pavel Raman...   EPM-SPI_Re...   [[Zabbix]_Pa...   MNT.NIX.EL...   1 / 4