
docker-compose-elasticsearch-kibana

Overview

Docker Compose for 3 Node Elasticsearch Cluster and Kibana Instance for development purposes.

- ☒ 3 Node Elasticsearch version
- ☒ Kibana version
- ☒ Audit Beat version
- ☒ Metric Beat version
- ☒ Heart Beat version
- ☒ Packet Beat version
- ☒ File Beat version
- ☒ APM Server version
- ☒ APM Search
- ☒ NGINX

NOTES

- If you need Open Source version then change Elasticsearch and Kibana Images to elasticsearch-oss and kibana-oss respectively.
- Kibana is being served behind Nginx Proxy so you can secure access of kibana for your purpose.

COMING UP DOCKER APPLICATION PACKAGE FOR SWARM

Requirements

- ☒ Docker 18.05
- ☒ Docker-compose 1.21

Start Stack in Daemon Mode

```
1 docker-compose up -d
```

Check status of docker-compose cluster

```
1 docker-compose ps -a
```

```
[[mpatel@MPATEL-M2231 ~/Mayank/Personal_Projects/docker-compose-elasticsearch-kibana/configs]$ docker ps -a
CONTAINER ID        IMAGE                                     COMMAND                  CREATED             STATUS              PORTS                               NAMES
45508e7418de        docker.elastic.co/app/am-server:7.0.0  "/usr/local/bin/dock..." About a minute ago  Up About a minute  0.0.0.0:8200->8200/tcp, 0.0.0.0:8201->8200/tcp  docker-compose-elasticsearch-kibana_apmservice_1
0d5d891e17a5        docker.elastic.co/beats/filebeat:7.0.0  "/usr/local/bin/dock..." About a minute ago  Up 56 seconds      0.0.0.0:9000->9000/tcp               docker-compose-elasticsearch-kibana_filebeat_1
944b327ed3e6        nginx:latest                           "bin/bash -c 'nginx..." About a minute ago  Up About a minute  0.0.0.0:8881->88/tcp                 docker-compose-elasticsearch-kibana_nginx_1
c93a50988a50        docker.elastic.co/elasticsearch/elasticsearch:7.0.0  "/usr/local/bin/dock..." About a minute ago  Up About a minute  0.0.0.0:9200->9200/tcp, 0.0.0.0:9300->9300/tcp  elasticsearch1
5a35820e0cf3        docker.elastic.co/beats/packetbeat:7.0.0  "/usr/local/bin/dock..." About a minute ago  Up About a minute  9300/tcp, 0.0.0.0:9202->9200/tcp      docker-compose-elasticsearch-kibana_packetbeat_1
248cafb0b6ae        docker.elastic.co/elasticsearch/elasticsearch:7.0.0  "/usr/local/bin/dock..." About a minute ago  Up About a minute  9300/tcp, 0.0.0.0:9201->9200/tcp      elasticsearch2
b399e2a19f4e        docker.elastic.co/beats/auditbeat:7.0.0  "/usr/local/bin/dock..." About a minute ago  Up About a minute  9300/tcp, 0.0.0.0:9201->9200/tcp      docker-compose-elasticsearch-kibana_auditbeat_1
dde7348f5cb2        docker.elastic.co/beats/heartbeat:7.0.0  "/usr/local/bin/dock..." About a minute ago  Up About a minute  9300/tcp, 0.0.0.0:9201->9200/tcp      docker-compose-elasticsearch-kibana_heartbeat_1
8302e6213fb        docker.elastic.co/beats/metricbeat:7.0.0  "/usr/local/bin/dock..." About a minute ago  Up About a minute  0.0.0.0:5601->5601/tcp               kibana
29d221f3cfd        docker.elastic.co/kibana/kibana:7.0.0    "/usr/local/bin/kiba..." About a minute ago  Up About a minute  0.0.0.0:5601->5601/tcp               kibana
```

Stop Compose Stack

```
1 docker-compose down
```

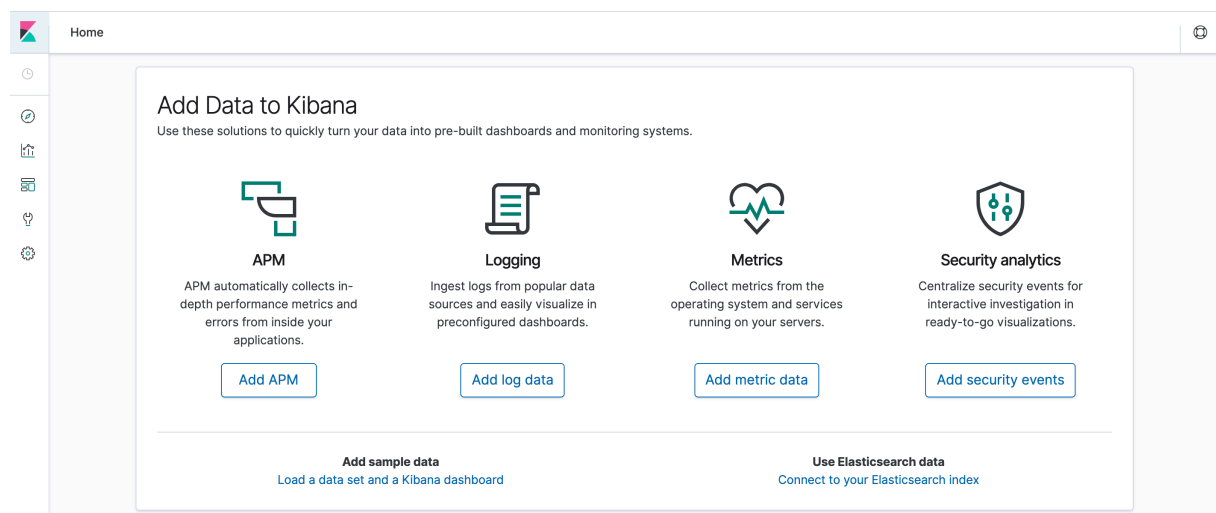
Cluster Node Info

```
1 curl http://localhost:9200/_nodes?pretty=true
```

Access Kibana

```
1 http://localhost:5601
```

Validate Kibana is running

The screenshot shows the Kibana Home page. At the top, there's a 'Home' header with a search icon. Below it, a large card titled 'Add Data to Kibana' provides instructions on using pre-built dashboards. This card contains four main sections: 'APM' (Add APM), 'Logging' (Add log data), 'Metrics' (Add metric data), and 'Security analytics' (Add security events). Each section has a brief description and a button to add the data. At the bottom of the card, there are two links: 'Add sample data' (Load a data set and a Kibana dashboard) and 'Use Elasticsearch data' (Connect to your Elasticsearch index).

Accessing Kibana through Nginx

```
1 http://localhost:8080
```

Access Elasticsearch

```
1 http://localhost:9200
```

Validate Elasticsearch is running

```
{
  "name": "3d5d14e27ed6",
  "cluster_name": "docker-cluster",
  "cluster_uuid": "YUjHiAMDQV6fiIMLVHD4UA",
  "version": {
    "number": "7.0.0",
    "build_flavor": "default",
    "build_type": "docker",
    "build_hash": "b7e28a7",
    "build_date": "2019-04-05T22:55:32.697037Z",
    "build_snapshot": false,
    "lucene_version": "8.0.0",
    "minimum_wire_compatibility_version": "6.7.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}
```

Raw Parsed

Resources

- [Hands on Elasticsearch](#)
- [Elasticsearch Resources](#)
- [Open Distro Elasticsearch](#)