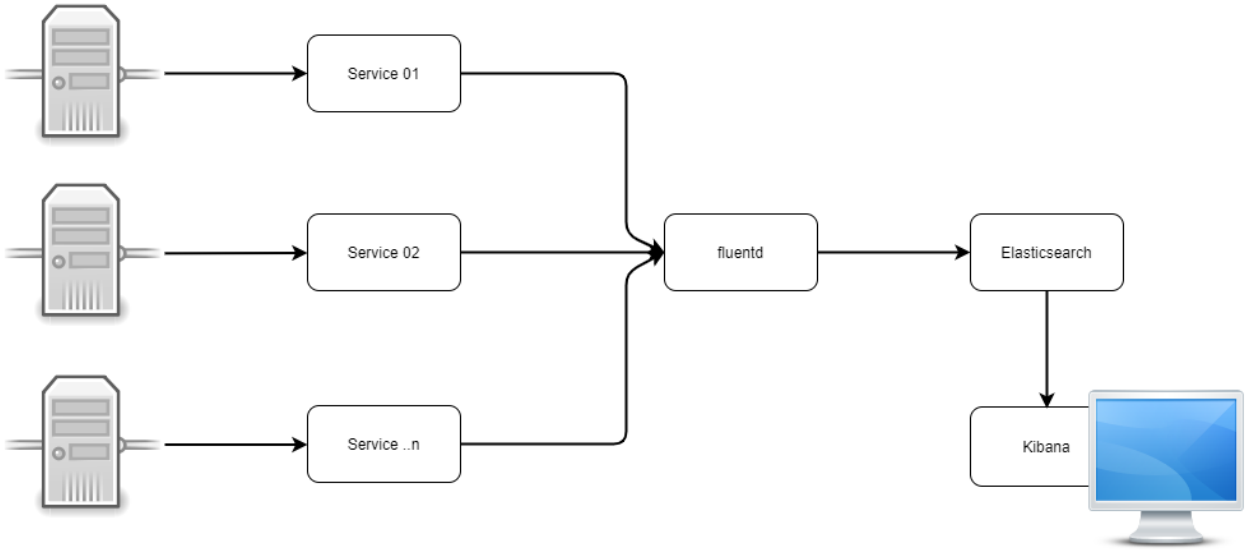
Centralized logging using EFK

Monolithic approach is a default model for creating a software application. A monolithic application is built as a single and indivisible unit which means implementation of logging is similar and only a single log file is enough.

Micro service is an idea to splits application into a set of smaller, interconnected services instead of building a single monolithic application. Every service called container and every container have separate logging. Most difficult part is to handle micro service log without any logging mechanism.

EFK is the solution to centralized logging for micro services and visualize it to users. EFK stand for elasticsearch, fluentd and Kibana.



- **Fluentd** gathers logs from nodes, clean and parse the log data and feeds them to elasticsearch
- **Elasticsearch** is a search and analytics engine for an object store where all logs are stored.
- **Kibana** is a web UI for elasticsearch. lets users visualize data with charts and graphs in Elasticsearch

Getting Started with EFK

Now have to learn some fundamental concepts of the EFK software that we are going to use, let's get start to deploy on window 10

Step1. Please click the link to download latest version of elasticsearch for your operating system. unzip folder in a selected drive

Step2. Access bin folder and run elasticsearch.bat in command prompt

```
C:\EFK\elasticsearch-7.6.2\bin>elasticsearch.bat
```

Elasticsearch is running and can be access using url http://127.0.0.1:9200

127.0.0.1:9200


```
{
  "name" : "LAPTOP-02QAHBFL",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "xcs0_O5ASbuI5ys0fOkNBg",
  "version" : {
    "number" : "7.6.2",
    "build_flavor" : "default",
    "build_type" : "zip",
    "build_hash" : "ef48eb35cf30adf4db14086e8aabd07ef6fb113f",
    "build_date" : "2020-03-26T06:34:37.794943Z",
    "build_snapshot" : false,
    "lucene_version" : "8.4.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```


Step3. Please click link to download latest version of kibana for your machine. Unzip folder

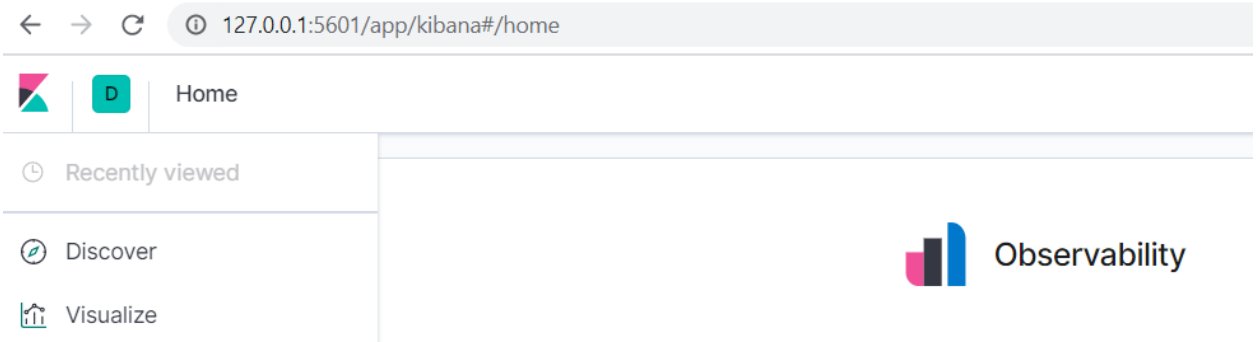
Step4. Go into kibana-7.6.2\config folder and edit kibana.yml. Uncomment elasticsearch.hosts

```
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]
```

Step5. Open command prompt and run kibana.bat

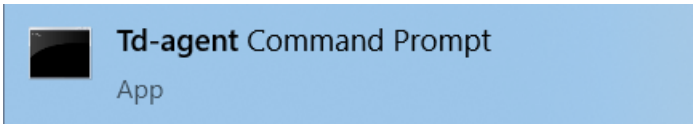
```
C:\EFK\kibana-7.6.2\bin>kibana.bat
log   [04:28:07.561] [info][server][Kibana][http] http server running at http://localhost:5601
```

Step6. Kibana running on port 5601 and can be access using url http://127.0.0.1:5601



Step7. Please click the link to download the latest version of fluentd and install it

Step8. Open td-agent command prompt and install fluent-plugin-elasticsearch




```
C:\opt\td-agent>fluent-gem install fluent-plugin-elasticsearch
```

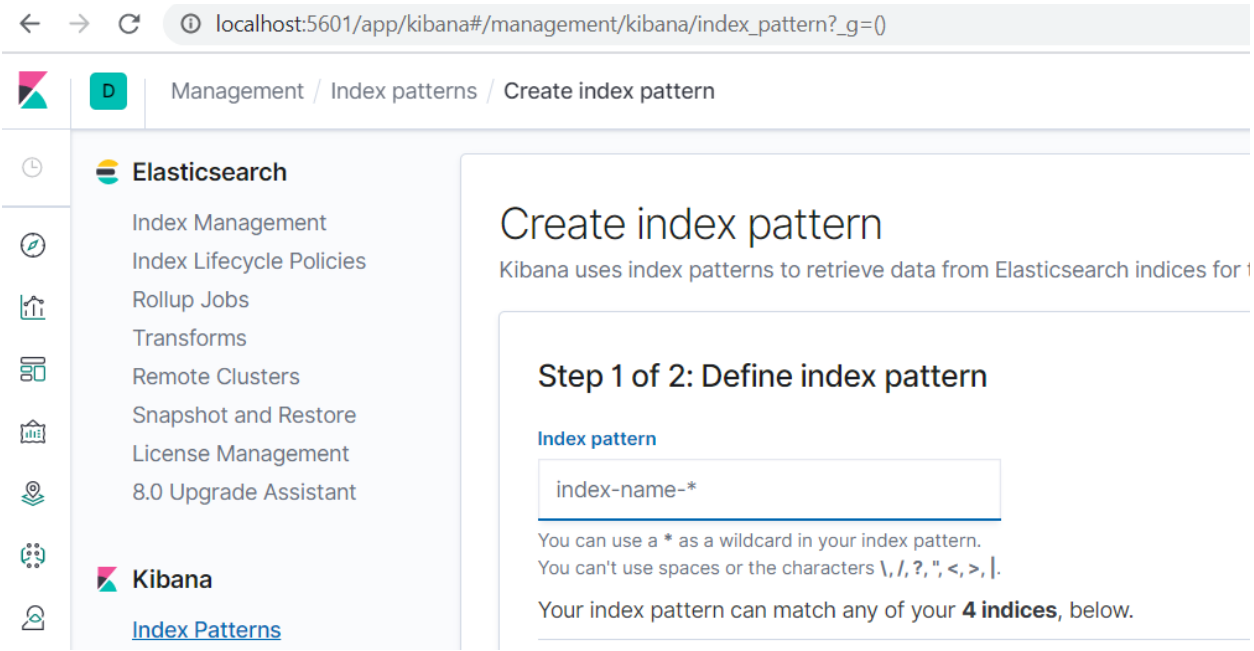
Step9. Access folder C:\opt\td-agent\etc\td-agent and open td-agent.conf into editor and modify td-agent.conf file as per below code

```
<source>
 @type forward
 port 24224
</source>
<match **>
 @type elasticsearch
 logstash_format true
 host localhost
 port 9200
 flush_interval 5s
</match>
```

Step10. In the prompt, please execute the command below to launch td-agent process

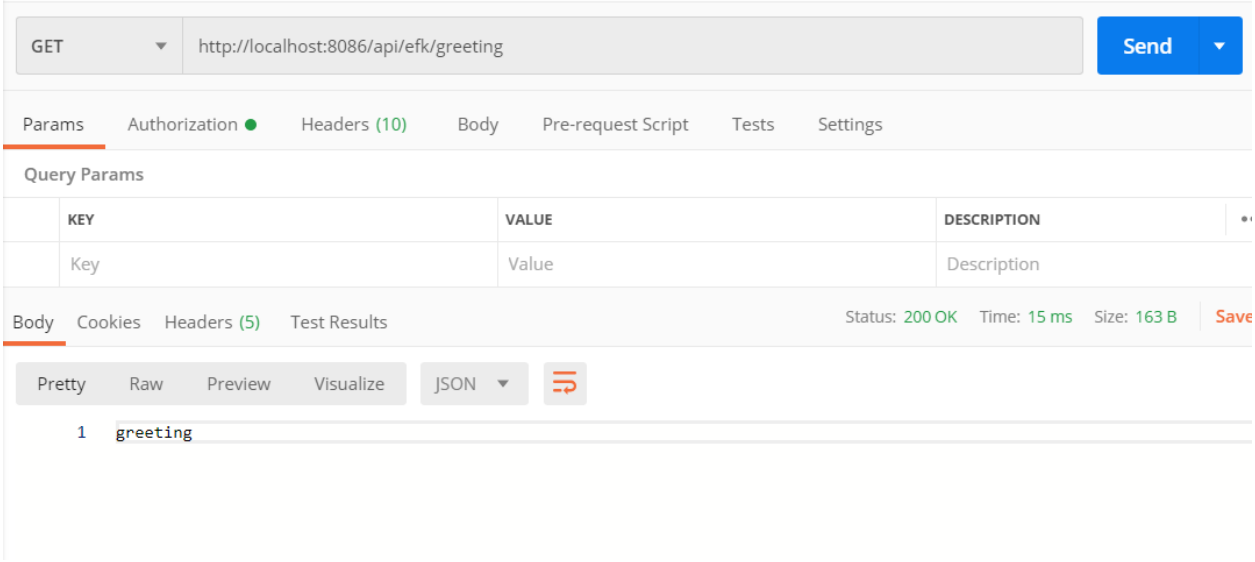
```
C:\opt\td-agent>fluentd -c etc\td-agent\td-agent.conf
listening port port=24224 bind="0.0.0.0"
fluentd worker is now running worker=0
```

Step11. Open kibana using url http://localhost:5601 and create new index pattern

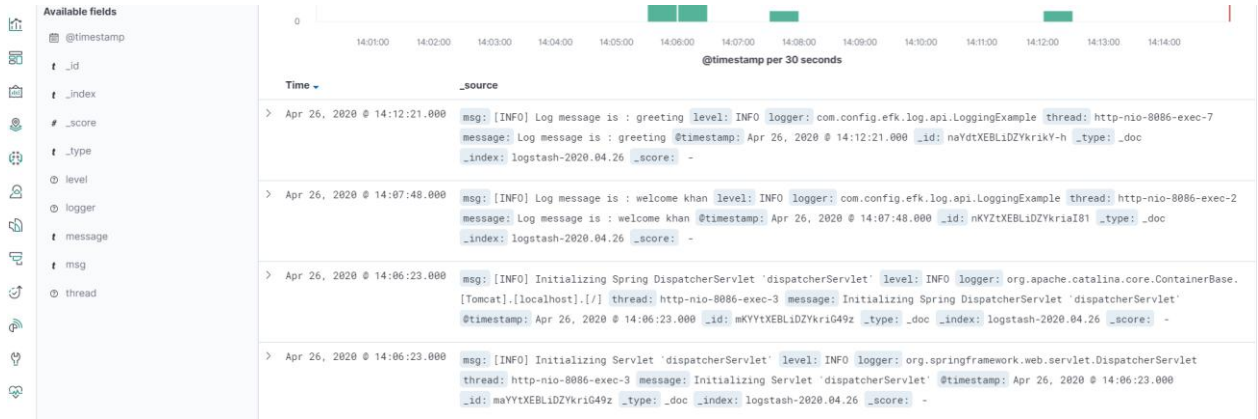


Step12. Please clone project folder centralized-logging-using-efk and run springboot application

Step13. Call api inside postman to generate log



Step14. Please access kibana dashboard and verify log



Conclusion

This article explains a basic implementation of EFK using single node on local machine. EFK know as platform services. It’s better to install EFK separate from application. My organization is using rancher configured with fluentd to send kubernates logs on elasticsearch