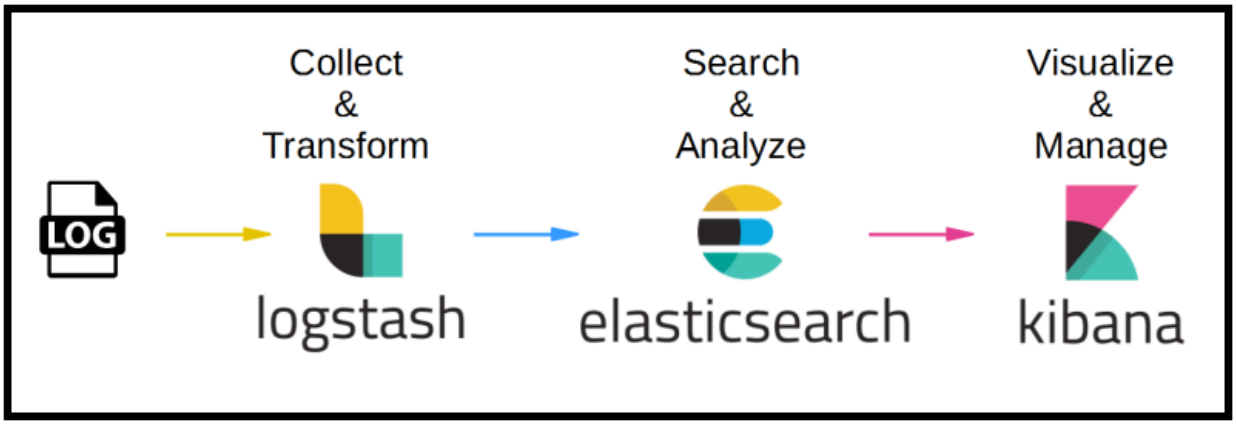
Mr. RAGHU [Naresh I Technologies, Ameerpet, Hyderabad, Telangana, India -500038

Spring Boot ELK - Mr. RAGHU



ELK Stack

1. **Elasticsearch** is a distributed, JSON-based *search and analytics engine* designed for horizontal scalability, maximum reliability, and easy management.
2. **Logstash** is a dynamic *data collection pipeline* with an extensible plug-in ecosystem and strong Elasticsearch synergy.
3. **Kibana** gives the *visualization* of data through a UI.

ELK stack configuration

Elasticsearch

A. Download latest version of Elasticsearch from this download **(https://www.elastic.co/downloads/elasticsearch)** page and unzip it any folder.
B. Run bin\elasticsearch.bat from command prompt.
C. By default, it would start at http://localhost:9200

Kibana

A. Download the latest distribution from download **(https://www.elastic.co/downloads/kibana)** page and unzip into any folder.
B. Open config/kibana.yml in an editor and set elasticsearch.hosts to point at your Elasticsearch instance. In our case as we will use the local instance just uncomment elasticsearch.hosts: "http://localhost:9200"
C. Run bin\kibana.bat from command prompt.

D. Once started successfully, Kibana will start on default port 5601 and Kibana UI will be available at http://localhost:5601

Logstash

A. Download the latest distribution from download **(https://www.elastic.co/downloads/logstash)** page and unzip into any folder.
B. Create one file logstash.conf as per configuration instructions **(https://www.elastic.co/guide/en/logstash/current/configuration.html)**.
C. Now run bin/logstash -f logstash.conf to start logstash

```
input {
  file {
    type => "java"
    path => "F:/mylogs/elktest.log"
    codec => multiline {
      pattern => "^%{YEAR}-%{MONTHNUM}-%{MONTHDAY} %{TIME}.*"
      negate => "true"
      what => "previous"
    }
  }
}

filter {
  if [message] =~ "\tat" {
    grok {
      match => ["message", "^(\tat)"]
      add_tag => ["stacktrace"]
    }
  }

}

output {
  stdout {
    codec => rubydebug
  }
  elasticsearch {
    hosts => ["localhost:9200"]
  }
}
```

Mr. RAGHU [Naresh I Technologies, Ameerpet, Hyderabad, Telangana, India -500038

Spring Boot Application

Name : SpringBootELKExample

Dependency: Spring Web

1. AppUtil.java

```
package in.nareshit.raghu.util;

import java.io.PrintWriter;
import java.io.StringWriter;

public interface AppUtil {

	public static String getLogSupport(Exception e) {
		StringWriter sw = new StringWriter();
		PrintWriter pw = new PrintWriter(sw);
		e.printStackTrace(pw);
		return  sw.toString();
	}

}
```

2. PaymentRestController.java

```
package in.nareshit.raghu.rest;

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import org.springframework.web.bind.annotation.GetMapping;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.RestController;

import in.nareshit.raghu.util.AppUtil;

@RestController
@RequestMapping("/payment")
public class PaymentRestController {

	private static final Logger LOG =
LoggerFactory.getLogger(PaymentRestController.class);

	@GetMapping("/doPay")
	public String doPayment() {
```

```
            LOG.info("ENTERED INTO PAYMENT SERVICE");
            try {
                 LOG.info("PAYMENT ABOUT TO START!");
                 throw new RuntimeException("INVALID OTP !");
            } catch (Exception e) {
                 e.printStackTrace();
                 LOG.error("PAYMENT ABOUT TO START!");
                 LOG.error("Exception - " +
AppUtil.getLogSupport(e));
            }
            return "SUCCESS";
      }


}
```

3. application.properties

```
logging.file.name=F:/mylogs/elktest.log
```

4. Start Project and Enter URL as: http://localhost:8080/payment/doPay

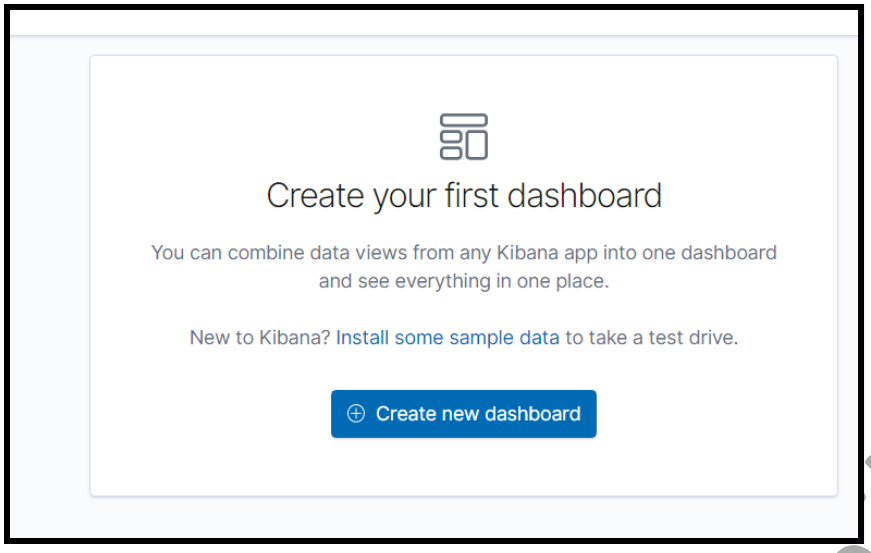
Check Log Lines

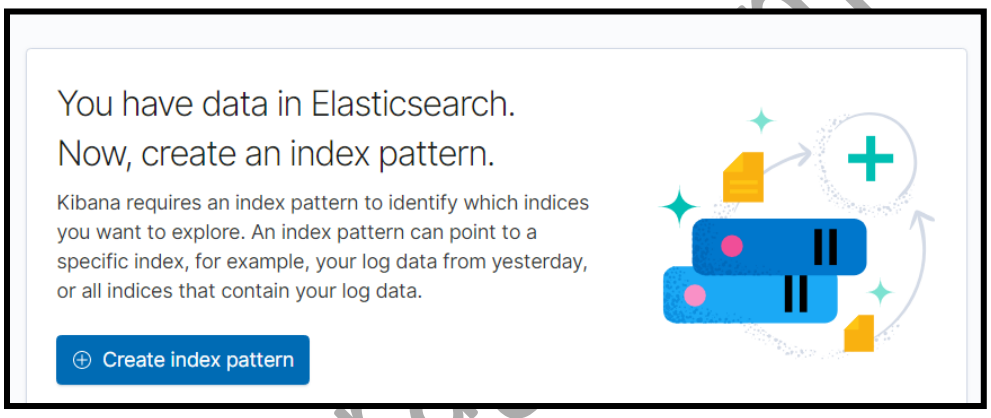
A. Goto Kibana UI http://localhost:5601

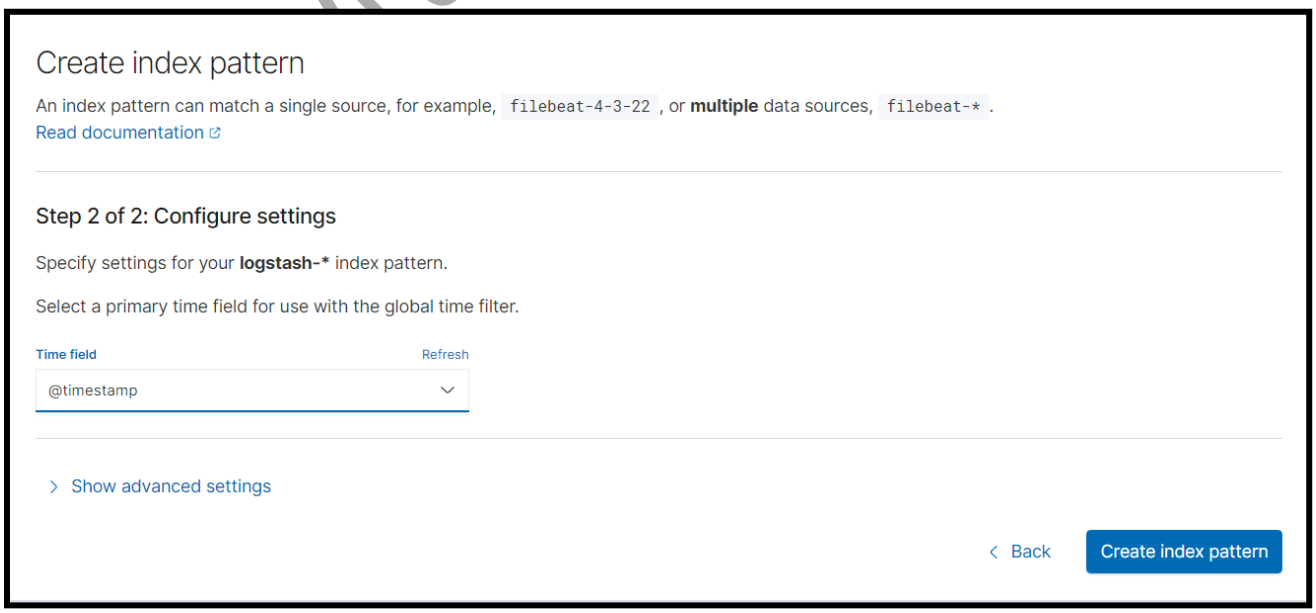
B. Click on DashBoard and choose Create new Dashboard

C. Click on Create New Index Pattern and Enter : logstash-* select @timestamp

D. Click on Discover Option and change Date Time for Search


Create your first dashboard
You can combine data views from any Kibana app into one dashboard and see everything in one place.
New to Kibana? Install some sample data to take a test drive.
Create new dashboard


You have data in Elasticsearch.
Now, create an index pattern.
Kibana requires an index pattern to identify which indices you want to explore. An index pattern can point to a specific index, for example, your log data from yesterday, or all indices that contain your log data.
Create index pattern


Create index pattern
An index pattern can match a single source, for example, filebeat-4-3-22 , or multiple data sources, filebeat-* .
Read documentation
Step 2 of 2: Configure settings
Specify settings for your logstash-* index pattern.
Select a primary time field for use with the global time filter.
Time field
Refresh
@timestamp
Show advanced settings
Back
Create index pattern

Mr. RAGHU [Naresh I Technologies, Ameerpet, Hyderabad, Telangana, India -500038