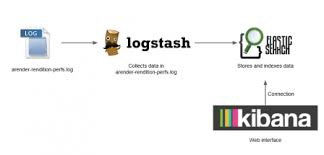
**ELK - Elastic Search, Logstash, Kibana**

ELK is a collection of tools from elastic to manage logs. The ELK stack is composed of 3 components:

**Elasticsearch**: This is a distributed search server. In this scenario is used to store log messages.

**Logstash**: Logstash is a tool for managing events and logs. When used generically the term encompasses a larger system of log collection, processing, storage and searching activities

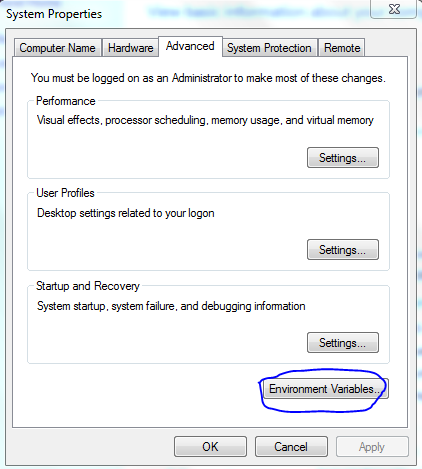
**Kibana**: It's a log analyzer (and eventually viewer) that allows to easily creating charts, stats and nice dashboards analyzing the log messages stored in elasticsearch.



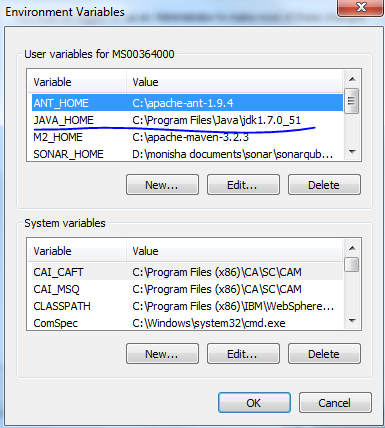
**Prerequisites**

* Java 7 or higher (set the JAVA\_HOME path)

-control panel🡪system and security🡪system🡪Advance system setting



Set the home path for java



* elasticsearch-2.1.1 (https://www.elastic.co/downloads/past-releases/elasticsearch-2-1-1)
* logstash-2.1.1 (https://www.elastic.co/downloads/past-releases/logstash-2-1-1)
* kibana-4.3.1 (<https://www.elastic.co/downloads/past-releases/kibana-4-3-1>)

**NOTE: there are two way of installation one is manual installation another is installation as service.so we can see both for all three (elasticsearch,logstash,kibana).you can prefer any one.**

1. **Download and Install Elastic Search**

**Manual installation:**

1. Download Elasticsearch zip file from the below location

<https://www.elastic.co/downloads/past-releases/elasticsearch-2-1-1>

1. Unzip and extract the content to the suitable directory

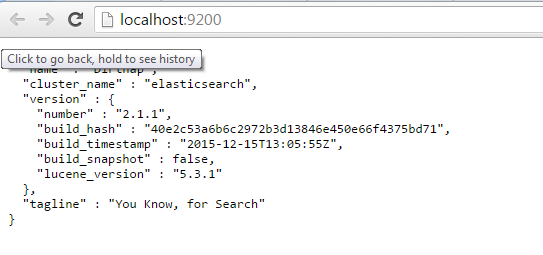
C:\elasticsearch-2.1.1

1. Go to the bin directory and start the server using command prompt

C:\elasticsearch-2.1.1\ bin\ elasticsearch.bat

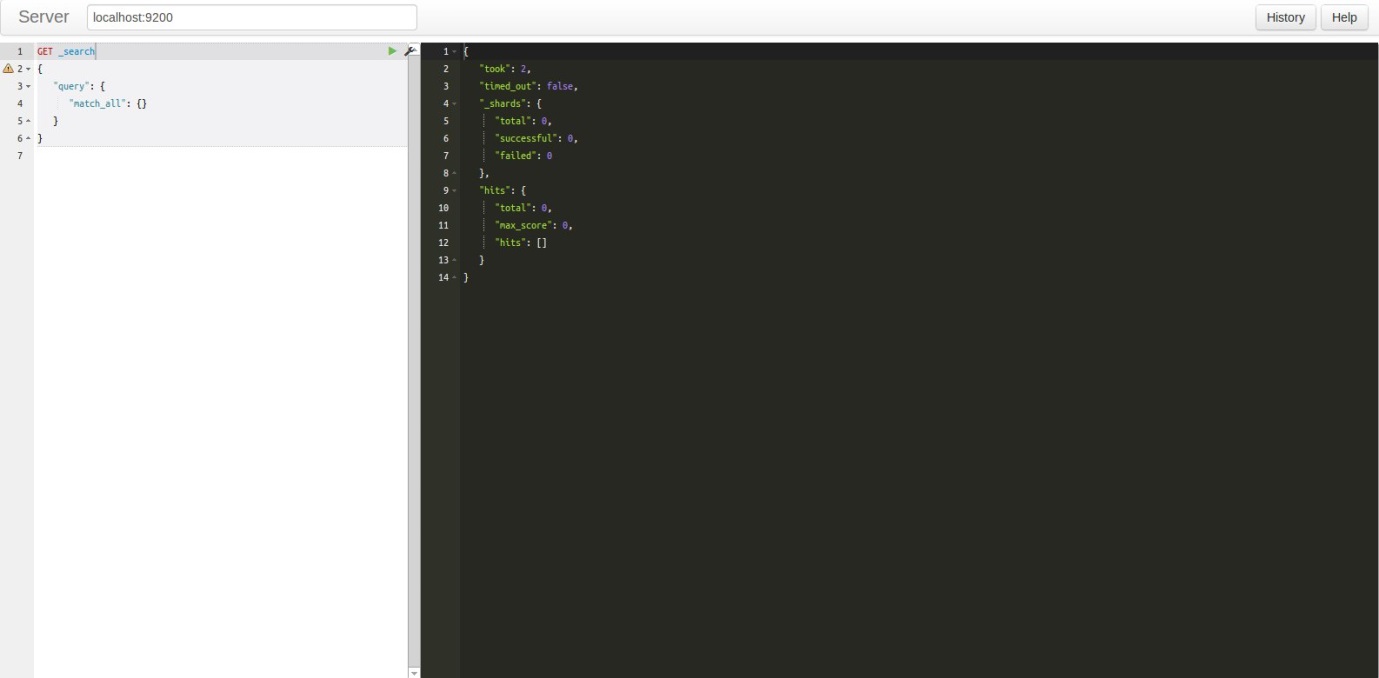
1. Make sure the elastic search is working.

<http://localhost:9200>



1. To work with elasticsearch we can use chrome plugins eg(Sense,postman..)

Here I am using sense –beta plugin(it’s a chrome add-on you can add It to you chrome)



Left side🡪write the query

Right side🡪see the result

In above we have written for search data where we didn’t get any output because we didn’t add any index to the elasticsearch.

1. **Download and Install Kibana Search**

**Manual Installation:**

1. Download zip file from the below location

<https://www.elastic.co/downloads/past-releases/kibana-4-3-1>

1. Unzip and extract the content to the suitable directory

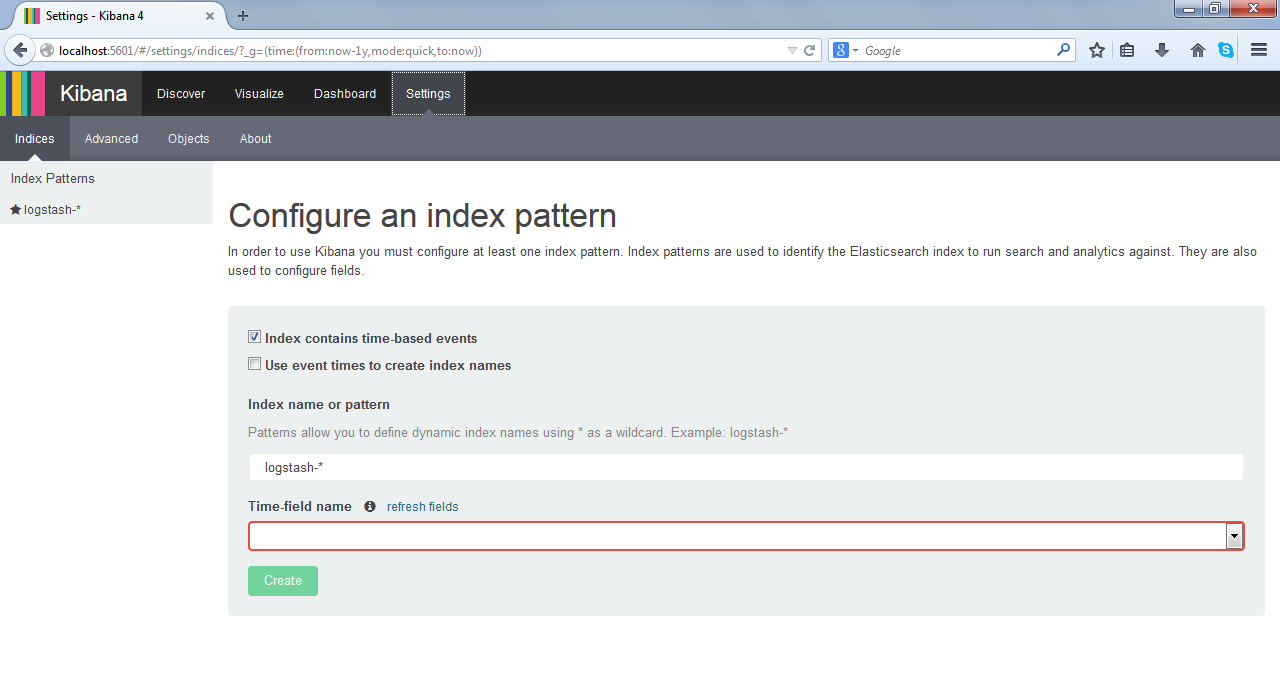
C: \kibana-4.3.1-windows\

1. Go to the bin directory and start the server using command prompt)

C: \kibana-4.3.1-windows\bin\kibana.bat

1. Check whether the kibana is working by

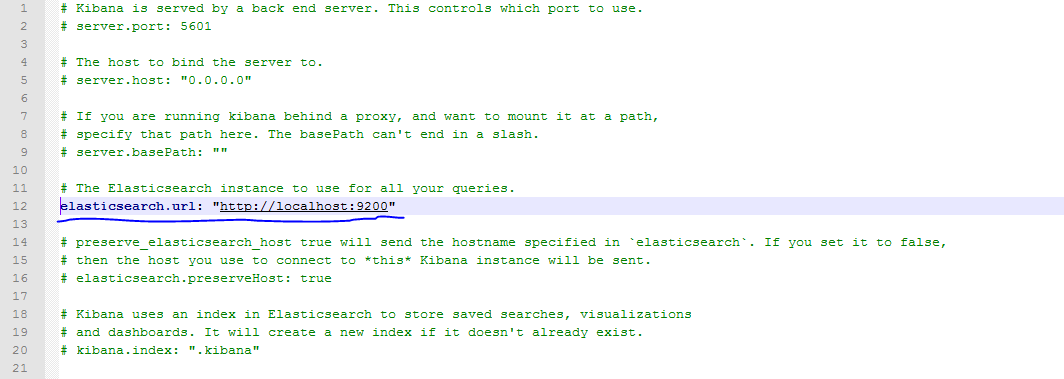
<http://localhost:5601/>



Kibana is working fine.

1. **Kibana Configuration with elasticsearch:**

Go to **C:\kibana\kibana-4.3.1-windows\config🡪**open the kibana.yml file and



Change the line as shown below

elasticsearch.url**:”**[**http://localhost:9200**](http://localhost:9200)**”** and save

Restart the kibana.bat file.now the elasticsearch is connected with kibana

1. **Download and Install Logstash**

**Manual installation:**

1. Download latest Logstash zip file from the below location

<https://www.elastic.co/downloads/past-releases/logstash-2-1-1>

1. Unzip and extract the content to the suitable directory

**C: \logstash-2.1.1**

1. Go to the bin directory

**C: \logstash-2.1.1\bin\**

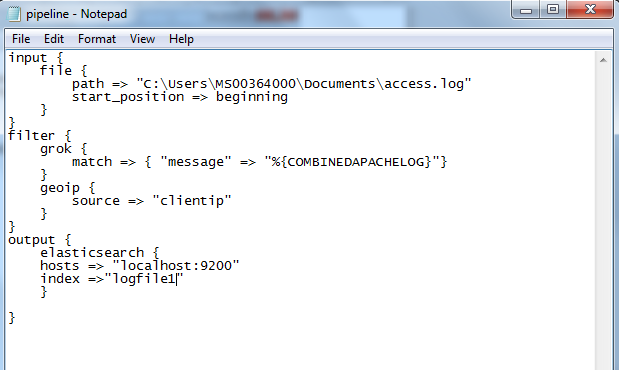
1. Before staring the logstash you should configure the logstash to elasticsearch.

So create a configuration file with the filter example: as shown below

**Input**: will have the log file path(**where you have the log file which you want to rear**)

**Filter**: will filter and index to the output

**Output**: should have the output path(where you want to store the data which you read from the logstash here it is elasticsearch)



Save the file as .conf file (eg:pipeline.conf) in logstash installation path.

Eg: C: \logstash-2.1.1\bin\

1. Then test the config file in command prompt(as admin)
2. **C: \logstash-2.1.1\bin>logstash –f pipeline.conf --configtest**

When you run it you will get the result as

Configuratoin OK

1. **C: \logstash-2.1.1\bin>logstash –f pipeline.conf (will run the conf file)**

Now the log from the log file will be read and will be stored in the elasticsearch.

Now you can check whether the data is getting stored in elasticsearch using sense plugin.

1. GET /\_cat/indices?v
2. POST /INDEX\_NAME/\_search?pretty' \_d'

{

"query":{"match\_all": {}},

"size":20

}

Now you can see the index(logfile1) is been created in the elasticsearch.