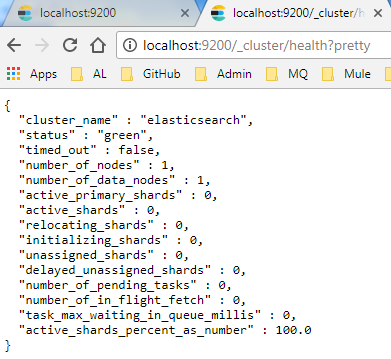
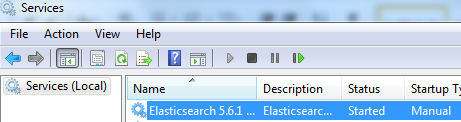
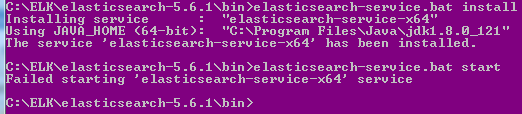
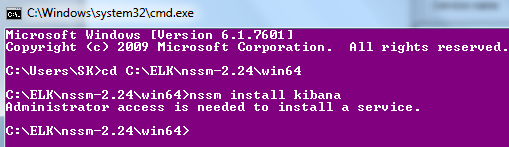
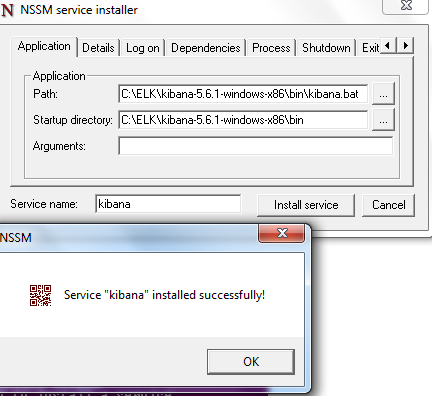
**ELK Stack using filebeats – NK 14/10/2017**

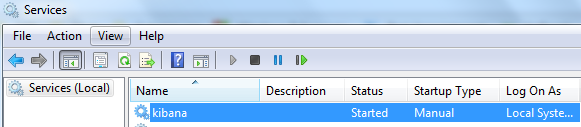
**Elastic search installation : http://localhost:9200/**



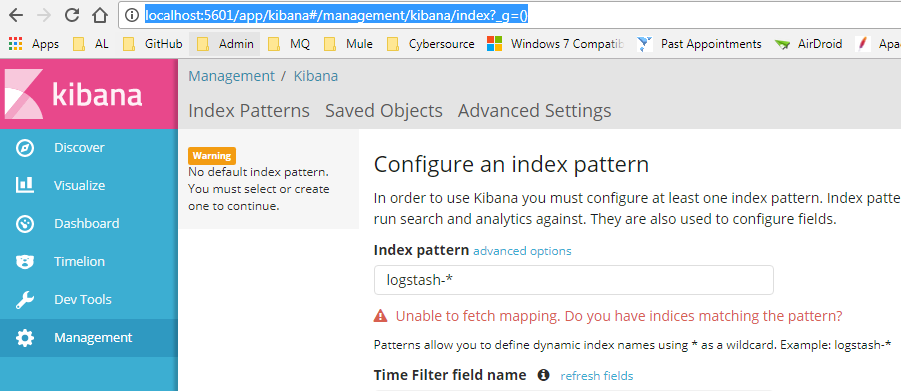
**Kibana installation**







[**http://localhost:5601/app/kibana#/management/kibana/index?\_g=()**](http://localhost:5601/app/kibana#/management/kibana/index?_g=())



**Logstash installation**

**Config file**

**Location :: C:\ELK\logstash-5.6.1\bin**

input {

file {

path => 'C:/ELK/logs/\*'

}

}

output {

elasticsearch {

hosts => ["localhost:9200"]

index => "logstash-%{+YYYY.MM.dd}"

}

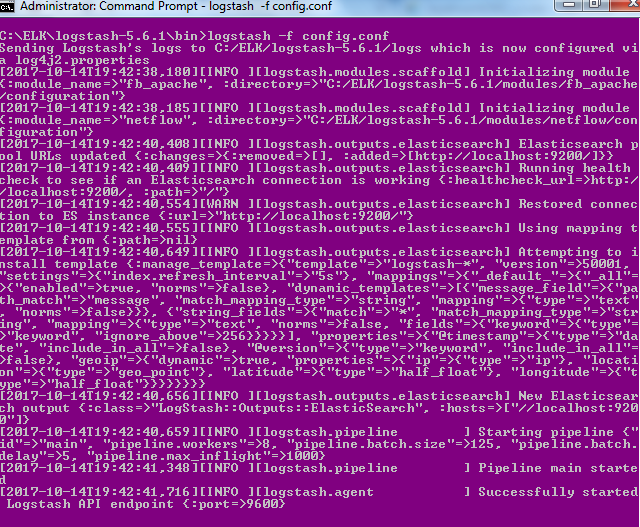
stdout { codec => rubydebug}

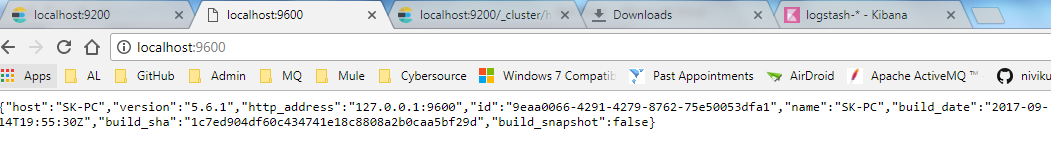
}

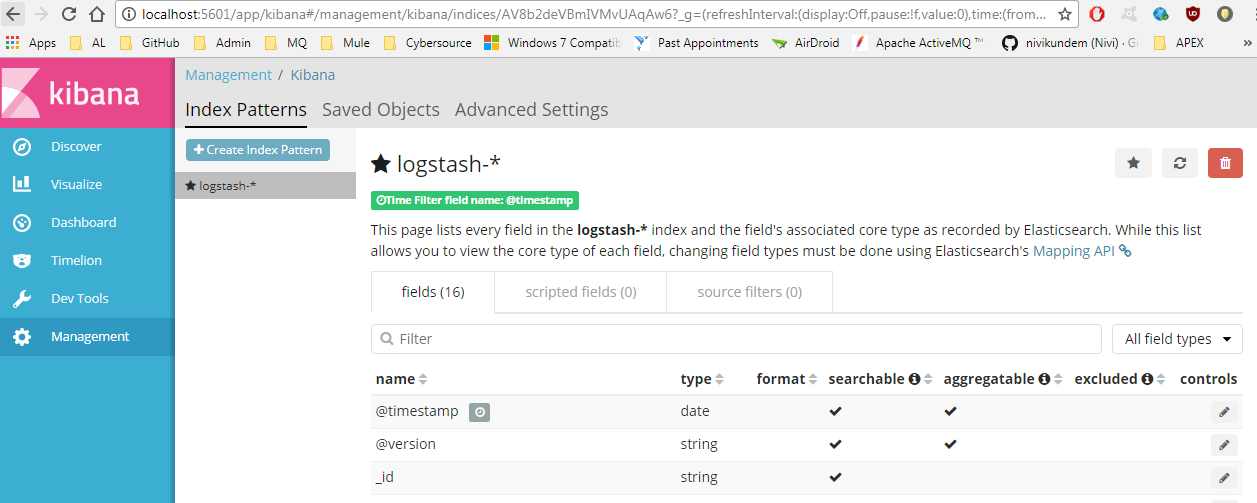
**To run ::**

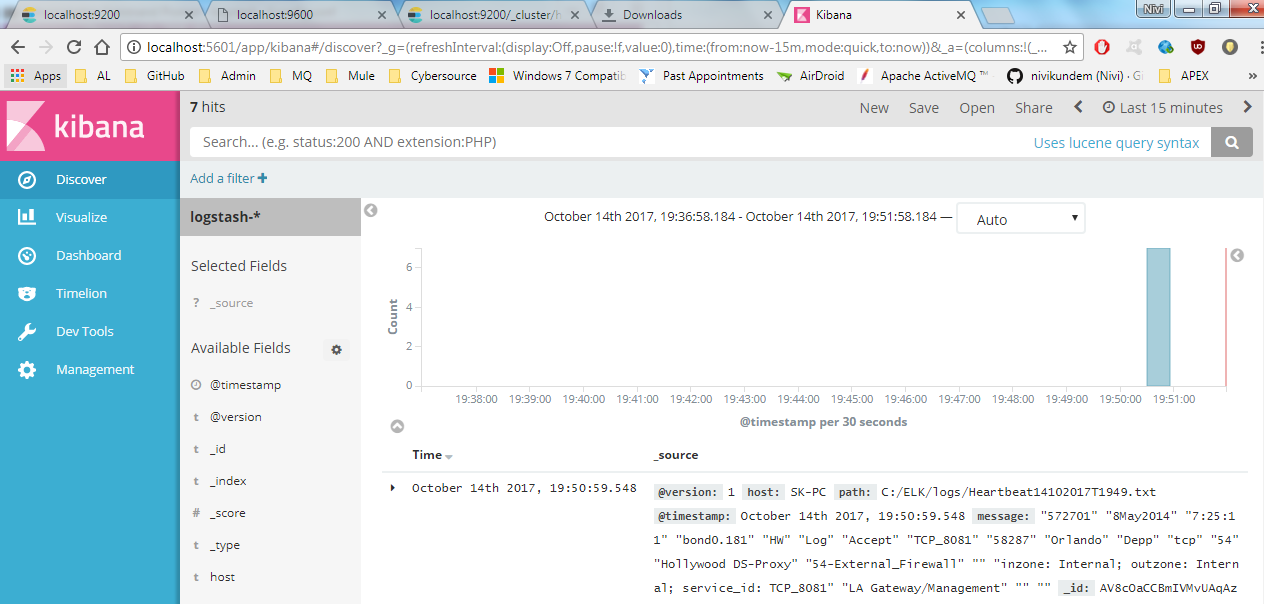
**C:\ELK\logstash-5.6.1\bin>logstash -f config.conf**

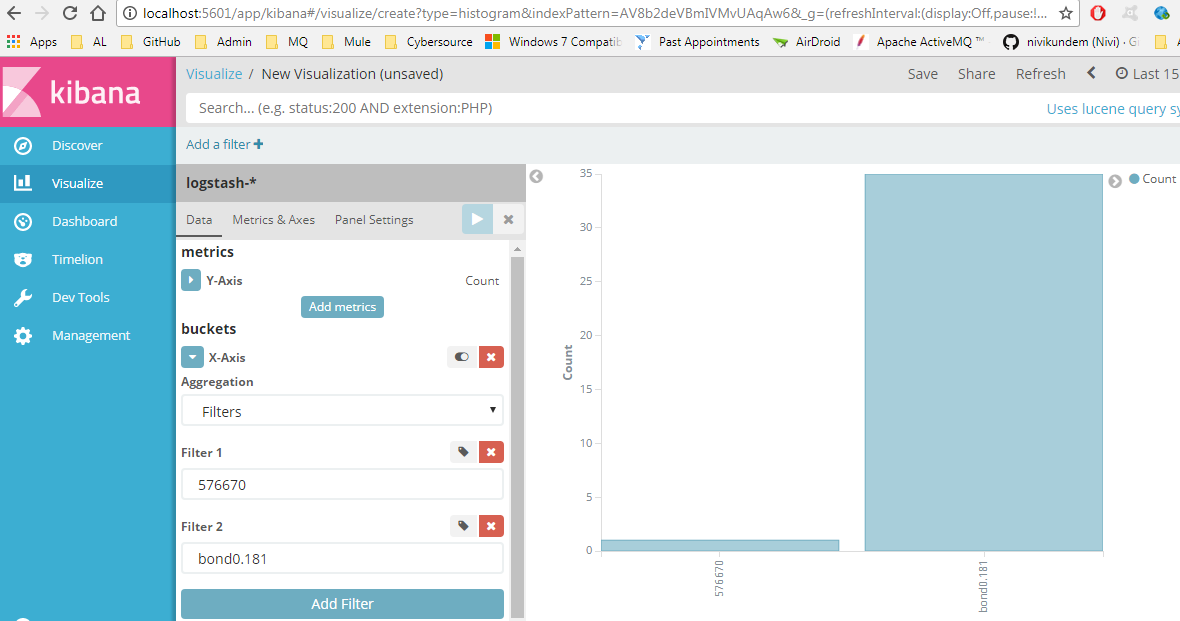
**logstash -f config.conf**











**Installing filebeat**

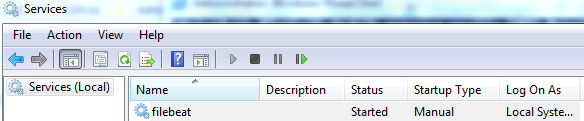
**Unzipped filebeat and change the folder name to Filebeat and copy to the** 'C:\Program Files

In powershell

PS > cd 'C:\Program Files\Filebeat'

PS C:\Program Files\Filebeat> .\install-service-filebeat.ps1

If script execution is disabled on your system, you need to set the execution policy for the current session to allow the script to run. For example: PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1



**To configure filebeat to the logstash**

In C:\Program Files\Filebeat in filebeat.yml

**Declare input location like below**

paths:

#- /var/log/\*.log

#- c:\programdata\elasticsearch\logs\\*

- c:\ELK\logsForFilebeat\\*

**Output location like below**

#-------------------------- Elasticsearch output ------------------------------

#output.elasticsearch:

# Array of hosts to connect to.

#hosts: ["localhost:9200"]

# Optional protocol and basic auth credentials.

#protocol: "https"

#username: "elastic"

#password: "changeme"

#----------------------------- Logstash output --------------------------------

output.logstash:

# The Logstash hosts

hosts: ["localhost:5044"]

**Configure Logstash to listen from the filebeat**

**For that we need to change the**

**Config file in the**

**Location :: C:\ELK\logstash-5.6.1\bin to below**

input {

beats {

port => 5044

}

}

output {

elasticsearch {

hosts => ["localhost:9200"]

index => "logstash-%{+YYYY.MM.dd}"

}

stdout { codec => rubydebug}

}

Need to restart

- Kibana service

- Elastic search service

- logstash from the cmd :: logstash -f config.conf



- filebeat service

