ELK: ELASTICSEARCH LOGSTASH KIBANA

INTRODUCTION / RUN BOOK

TO MONITOR

LOGS

Why ELK ?

ELK i.e **E**lasticsearch **L**ogstash **K**ibana is a collection of open-source software It allows you to collect analyze, and visualize logs generated from any source in any format, this concept also called as centralized logging. Centralized logging can help us to identify problems with our servers or applications, as it allows us to search through all of our logs in a single place and it allows to identify issues that span multiple servers by correlating their logs during a specific time frame.

Elasticsearch is a free and open source software. It allows you to store, search, and analyze big volumes of data quickly and in near real time.

Logstash will collect the data of the server and provide it to elastics search.

Once data reaches to elasticsearch, we can check all the logs.

It will process the data i.e send the data to elastic-search.

Kibana is dashboard where we can see the logs & metrics of the server in better visualized form with the help of elastic-search.

Installion Steps:-

Check java version by command **(java is required)**

```
# java -version
```

Download   Process Elastic search rpm file

```
# sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

Create Repo:

```
# sudo vi /etc/yum.repos.d/elasticsearch.repo
```

Add this in repo

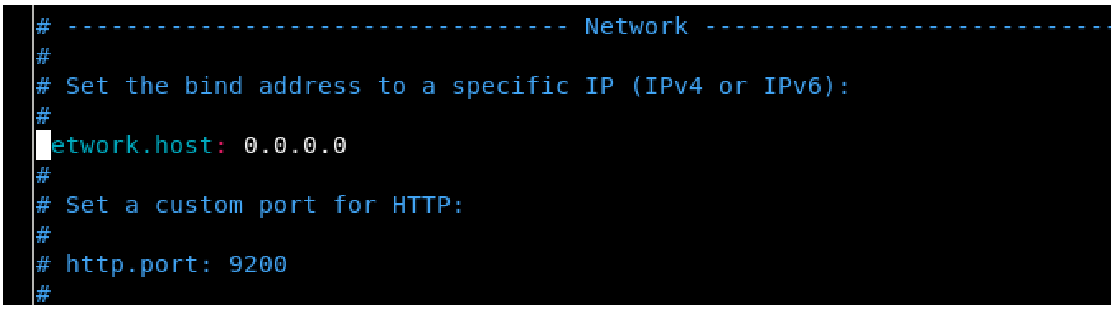
```
[elasticsearch-6.x]
name=Elasticsearch repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Install elasticsearch now

```
# sudo yum install elasticsearch
# sudo systemctl enable elasticsearch.service
```

Go to sudo vi /etc/elasticsearch/elasticsearch.yml and Configures the Elasticsearch server settings.

We can give IP/LOCALHOST/0.0.0.0 for local system



```
# ---------------------------------- Network -----------------------------
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
etwork.host: 0.0.0.0
#
# Set a custom port for HTTP:
#
# http.port: 9200
#
```

Remove the # character at the beginning of the lines for network host to uncomment them

Now start service by using follwoing command.

```
# sudo service elasticsearch start
```

```
# curl -X GET 'http://localhost:9200 OR in Browser
http://localhost:9200---After this command you should see this output-->
```

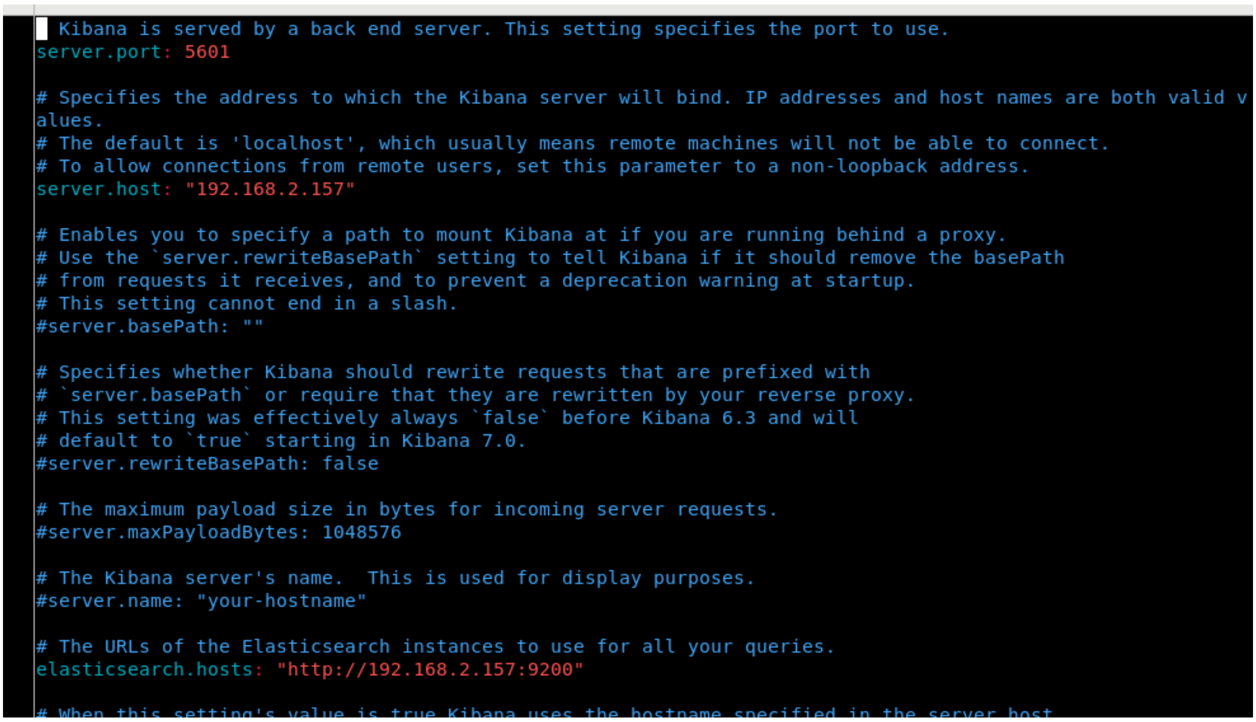
```
{
  "name" : "8oSCBFJ",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "1Nf9ZymBQaOWKpMRBfisog",
  "version" : {
    "number" : "6.5.2",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "9434bed",
    "build_date" : "2018-11-29T23:58:20.891072Z",
    "build_snapshot" : false,
    "lucene_version" : "7.5.0",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Installing and Configuring the Kibana Dashboard

```
# sudo yum install kibana
```

Configure kibana.yml file

- **# vi /etc/kibana/kibana.yml**

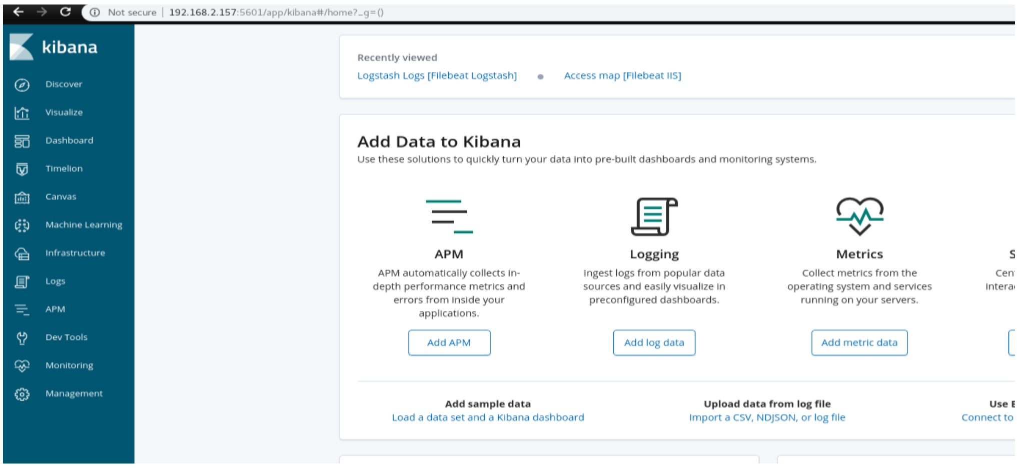


```
█ Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid v
alues.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "192.168.2.157"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# The maximum payload size in bytes for incoming server requests.
#server.maxPayloadBytes: 1048576

# The Kibana server's name.  This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: "http://192.168.2.157:9200"

# When this setting's value is true Kibana uses the hostname specified in the server.host
```

Uncomment this three lines. As per image.

sudo systemctl start kibana

Go to browser and http://your_server_ip:5601



Not secure | 192.168.2.157:5601/app/kibana#/home?_g=()

Recently viewed

Logstash Logs [Filebeat Logstash] • Access map [Filebeat IIS]

Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

Add metric data

S

Cen
intera

Add sample data

Load a data set and a Kibana dashboard

Upload data from log file

Import a CSV, NDJSON, or log file

Use E

Connect to

Installing and Configuring Logstash

- # sudo yum install logstash

Create a configuration file called 02-beats-input.conf where you will set up your Filebeat input:

- # sudo vi /etc/logstash/conf.d/02-beats-input.conf

Then add this.

```
input {

    beats {

        port => 5044

    }

}
```

Insert the following syslog filter configuration

- # sudo vi /etc/logstash/conf.d/10-syslog-filter.conf

Add this configuration.This filter is used to parse incoming system logs to make them structured and usable by the predefined Kibana dashboards

```
filter {

    if [fileset][module] == "system" {

        if [fileset][name] == "auth" {

            grok {

                match => { "message" => ["%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %{SYSLOGHOST:[system][auth][hostname]}
sshd(?:\[%{POSINT:[system][auth][pid]}\])?: %{DATA:[system][auth][ssh][event]} %{DATA:[system][auth][ssh][method]} for (invalid
user )?%{DATA:[system][auth][user]} from %{IPORHOST:[system][auth][ssh][ip]} port %{NUMBER:[system][auth][ssh][port]}
ssh2(: %{GREEDYDATA:[system][auth][ssh][signature]})?",

                                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %{SYSLOGHOST:[system][auth][hostname]}
sshd(?:\[%{POSINT:[system][auth][pid]}\])?: %{DATA:[system][auth][ssh][event]} user %{DATA:[system][auth][user]}
from %{IPORHOST:[system][auth][ssh][ip]}",

                                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %{SYSLOGHOST:[system][auth][hostname]}
sshd(?:\[%{POSINT:[system][auth][pid]}\])?: Did not receive identification string from %{IPORHOST:[system][auth][ssh][dropped_ip]}",

                                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %{SYSLOGHOST:[system][auth][hostname]}
sudo(?:\[%{POSINT:[system][auth][pid]}\])?: \s*%{DATA:[system][auth][user]} :( %{DATA:[system][auth][sudo][error]} ;)?
TTY=%{DATA:[system][auth][sudo][tty]} ; PWD=%{DATA:[system][auth][sudo][pwd]} ; USER=%{DATA:[system][auth][sudo][user]} ;
COMMAND=%{GREEDYDATA:[system][auth][sudo][command]}",

                                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %{SYSLOGHOST:[system][auth][hostname]}
groupadd(?:\[%{POSINT:[system][auth][pid]}\])?: new group: name=%{DATA:system.auth.groupadd.name},
GID=%{NUMBER:system.auth.groupadd.gid}",

                                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %{SYSLOGHOST:[system][auth][hostname]}
useradd(?:\[%{POSINT:[system][auth][pid]}\])?: new user: name=%{DATA:[system][auth][user][add][name]},
UID=%{NUMBER:[system][auth][user][add][uid]}, GID=%{NUMBER:[system][auth][user][add][gid]},
home=%{DATA:[system][auth][user][add][home]}, shell=%{DATA:[system][auth][user][add][shell]}$",


"%{SYSLOGTIMESTAMP:[system][auth][timestamp]} %{SYSLOGHOST:[system][auth][hostname]} %{DATA:[system][auth][program]}(?:\[%
{POSINT:[system][auth][pid]}\])?: %{GREEDYMULTILINE:[system][auth][message]}"] }

                pattern_definitions => {

                    "GREEDYMULTILINE"=> "(.|\n)*"
                }
                remove_field => "message"
            }
            date {
                match => [ "[system][auth][timestamp]", "MMM    d HH:mm:ss", "MMM dd HH:mm:ss" ]
            }
            geoip {
                source => "[system][auth][ssh][ip]"
                target => "[system][auth][ssh][geoip]"
            }
        }
        else if [fileset][name] == "syslog" {
            grok {
                match => { "message" =>
["%{SYSLOGTIMESTAMP:[system][syslog][timestamp]} %{SYSLOGHOST:[system][syslog][hostname]} %{DATA:[system][syslog][program]}(
?:\[%{POSINT:[system][syslog][pid]}\])?: %{GREEDYMULTILINE:[system][syslog][message]}"] }
                pattern_definitions => { "GREEDYMULTILINE" => "(.|\n)*" }
                remove_field => "message"
            }
            date {
                match => [ "[system][syslog][timestamp]", "MMM    d HH:mm:ss", "MMM dd HH:mm:ss" ]
            }
        }
    }
}
```

Now **Lastly, create a configuration file called 30-elasticsearch-output.conf:**

```
# sudo vi /etc/logstash/conf.d/30-elasticsearch-output.conf
```

Insert this:-

```
output {
    elasticsearch {
        hosts => ["localhost:9200"]
        manage_template => false
        index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
    }
}
```

# sudo systemctl start logstash

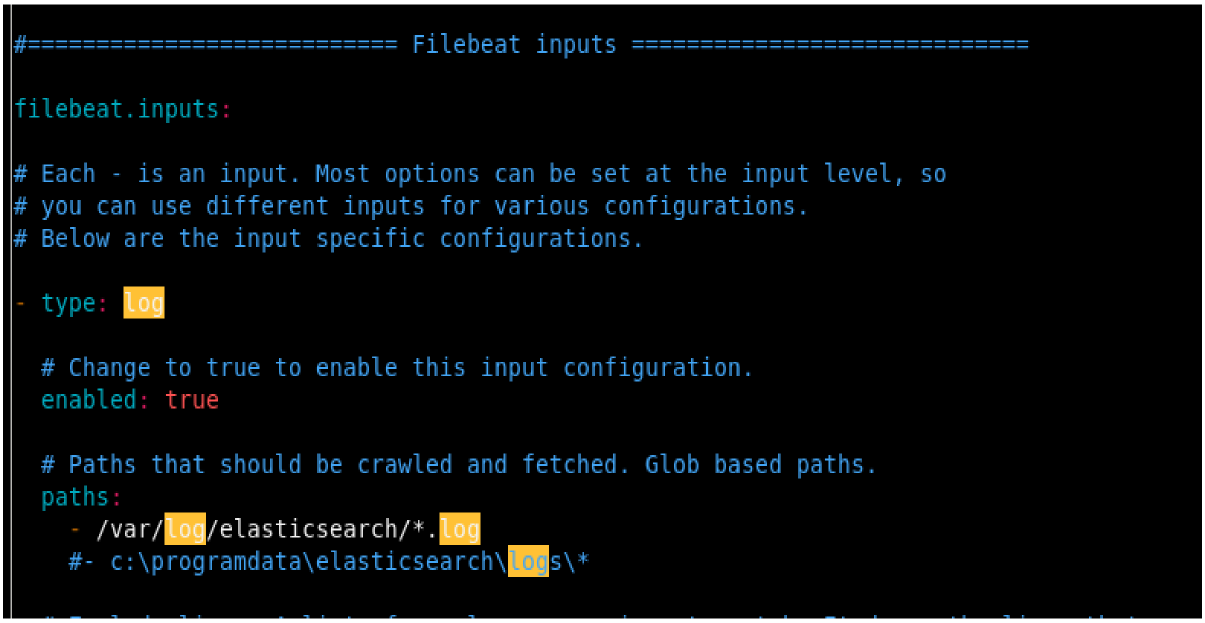
- # sudo systemctl enable logstash

Installing and Configuring Filebeat

- # sudo yum install filebeat

Now configure as bellow logstash to connect with logstash

- # sudo vi /etc/filebeat/filebeat.yml
- **Set type:log as true and dont forget to give correct path as below:**



```
#=========================== Filebeat inputs =============================

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

- type: log

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/elasticsearch/*.log
    #- c:\programdata\elasticsearch\logs\*
```

```
#output.elasticsearch:

  # Array of hosts to connect to.

  #hosts: ["localhost:9200"]
```

Then, configure the output.logstash, remove #

```
output.logstash:

  # The Logstash hosts

  hosts: ["localhost:5044"]
```

Now start filebeat---

sudo filebeat modules enable system

Enable the module as per your logs requirement---

- sudo filebeat modules list
- sudo filebeat setup --template -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'

After executing last command Output should be like this:--Loaded index template

To check the version information.

- # sudo filebeat setup -e -E output.logstash.enabled=false -E output.elasticsearch.hosts=['localhost:9200'] -E setup.kibana.host=localhost:5601

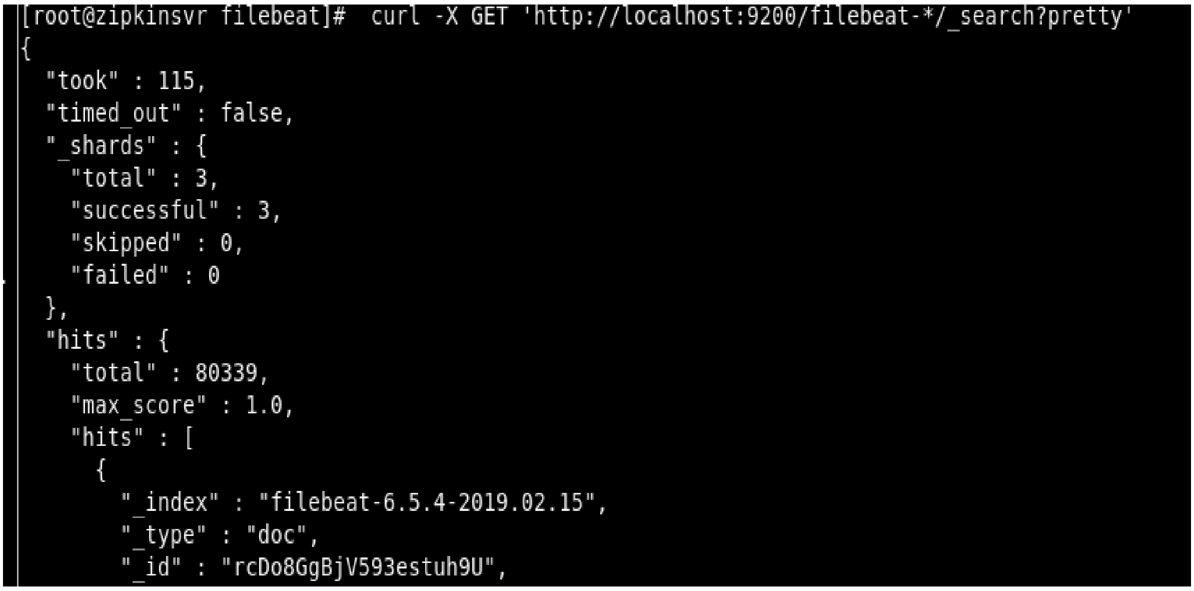
Now start the filebeat

- # sudo systemctl start filebeat

Then,

```
          # curl -X GET
'http://localhost:9200/filebeat-*/_search?pretty'
```

- **It should show hit numbers and successful numbers.**
- For example something like below:-



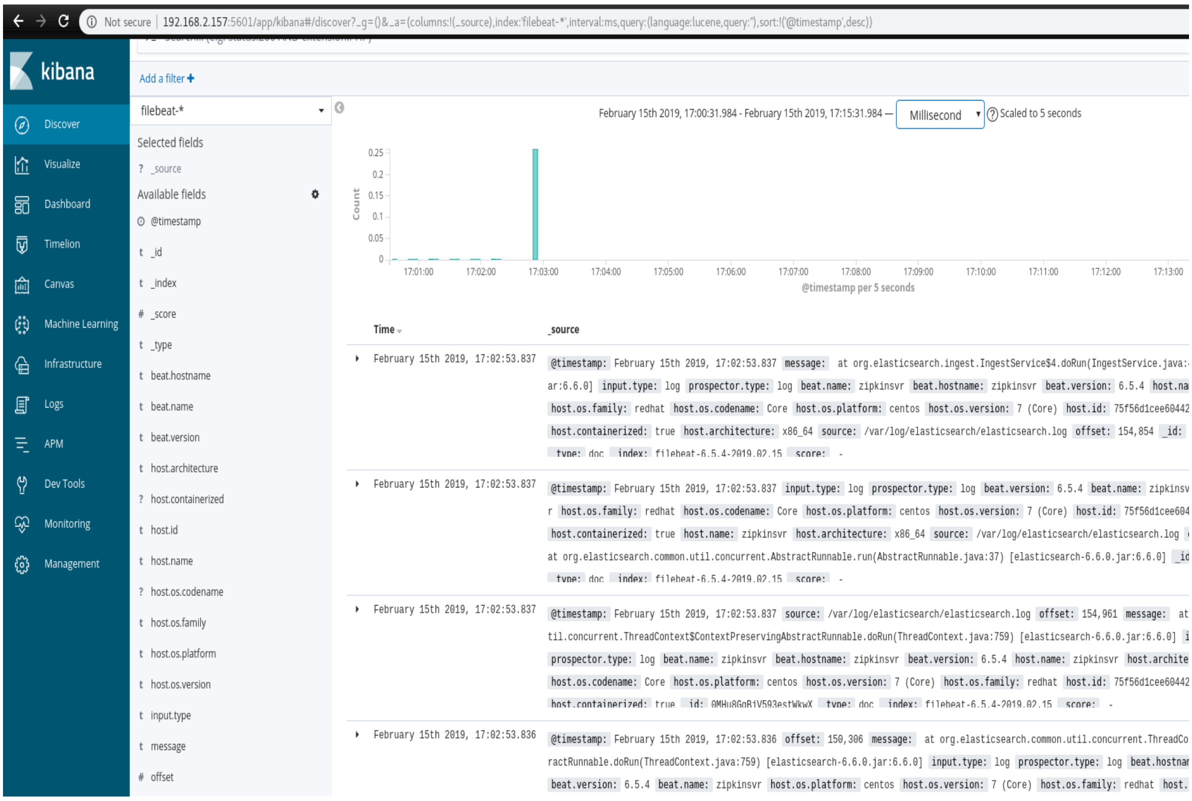
```
[root@zipkinsvr filebeat]#  curl -X GET 'http://localhost:9200/filebeat-*/_search?pretty'
{
  "took" : 115,
  "timed_out" : false,
  "_shards" : {
    "total" : 3,
    "successful" : 3,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : 80339,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "filebeat-6.5.4-2019.02.15",
        "_type" : "doc",
        "_id" : "rcDo8GgBjV593estuh9U",
```

Now Go to KIbana Dashboard http://localhost:5601/ OR IP:5601

Now click on **Discover**

Select **filebeat-* index**

Then it will show logs as below:-



```
192.168.2.157:5601/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:'filebeat-*',interval:ms,query:(language:lucene,query:''),sort:!('@timestamp',desc))
```

filebeat-*

February 15th 2019, 17:00:31.984 - February 15th 2019, 17:15:31.984 — Millisecond ▾ Scaled to 5 seconds

Selected fields

? _source

Available fields

@timestamp
t _id
t _index
_score
t _type
t beat.hostname
t beat.name
t beat.version
t host.architecture
? host.containerized
t host.id
t host.name
? host.os.codename
t host.os.family
t host.os.platform
t host.os.version
t input.type
t message
# offset

```
Time ▾                                 _source

February 15th 2019, 17:02:53.837       @timestamp: February 15th 2019, 17:02:53.837 message:  at org.elasticsearch.ingest.IngestService$4.doRun(IngestService.java:
                                       ar:6.6.0] input.type: log prospector.type: log beat.name: zipkinsvr beat.hostname: zipkinsvr beat.version: 6.5.4 host.na
                                       host.os.family: redhat host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.id: 75f56d1cee60442
                                       host.containerized: true host.architecture: x86_64 source: /var/log/elasticsearch/elasticsearch.log offset: 154,854 _id:
                                       _type: doc _index: filebeat-6.5.4-2019.02.15 _score: -

February 15th 2019, 17:02:53.837       @timestamp: February 15th 2019, 17:02:53.837 input.type: log prospector.type: log beat.version: 6.5.4 beat.name: zipkinsv
                                       r host.os.family: redhat host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.id: 75f56d1cee604
                                       host.containerized: true host.name: zipkinsvr host.architecture: x86_64 source: /var/log/elasticsearch/elasticsearch.log
                                       at org.elasticsearch.common.util.concurrent.AbstractRunnable.run(AbstractRunnable.java:37) [elasticsearch-6.6.0.jar:6.6.0] _id
                                       _type: doc _index: filebeat-6.5.4-2019.02.15 _score: -

February 15th 2019, 17:02:53.837       @timestamp: February 15th 2019, 17:02:53.837 source: /var/log/elasticsearch/elasticsearch.log offset: 154,961 message:  at
                                       til.concurrent.ThreadContext$ContextPreservingAbstractRunnable.doRun(ThreadContext.java:759) [elasticsearch-6.6.0.jar:6.6.0] i
                                       prospector.type: log beat.name: zipkinsvr beat.hostname: zipkinsvr beat.version: 6.5.4 host.name: zipkinsvr host.archite
                                       host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.os.family: redhat host.id: 75f56d1cee60442
                                       host.containerized: true _id: 0MHu8GqBiV593estWkwX _type: doc _index: filebeat-6.5.4-2019.02.15 _score: -

February 15th 2019, 17:02:53.836       @timestamp: February 15th 2019, 17:02:53.836 offset: 150,306 message:  at org.elasticsearch.common.util.concurrent.ThreadCo
                                       ractRunnable.doRun(ThreadContext.java:759) [elasticsearch-6.6.0.jar:6.6.0] input.type: log prospector.type: log beat.hostnar
                                       beat.version: 6.5.4 beat.name: zipkinsvr host.os.platform: centos host.os.version: 7 (Core) host.os.family: redhat host.
```

****