**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

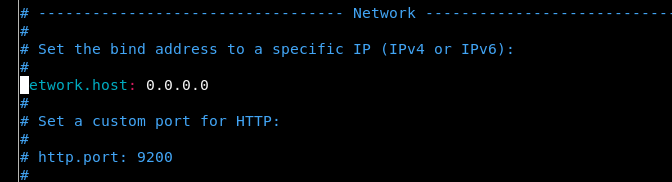
**Install elasticsearch now**

# 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



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"

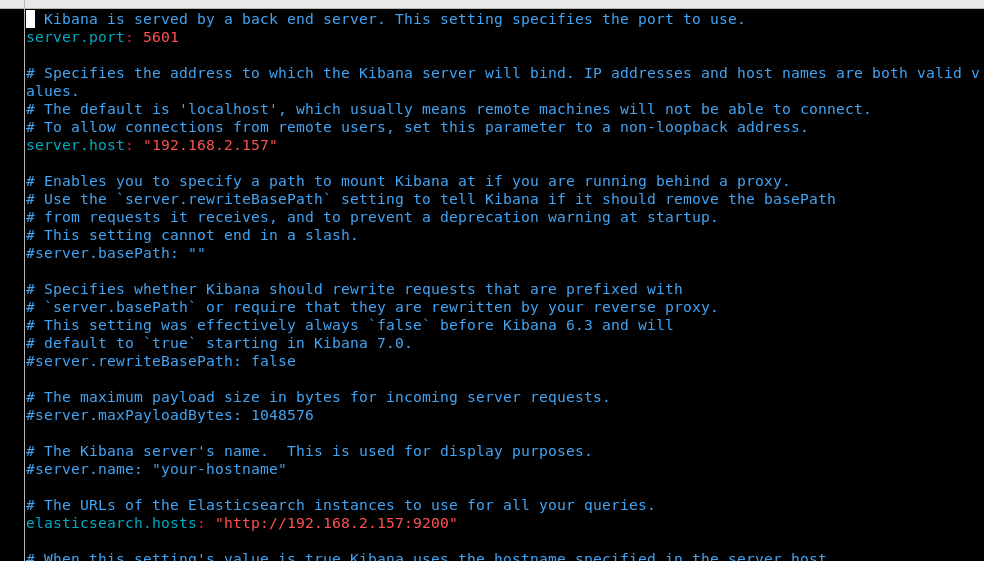
}

**Installing and Configuring the Kibana Dashboard**

# sudo yum install kibana

**Configure kibana.yml file**

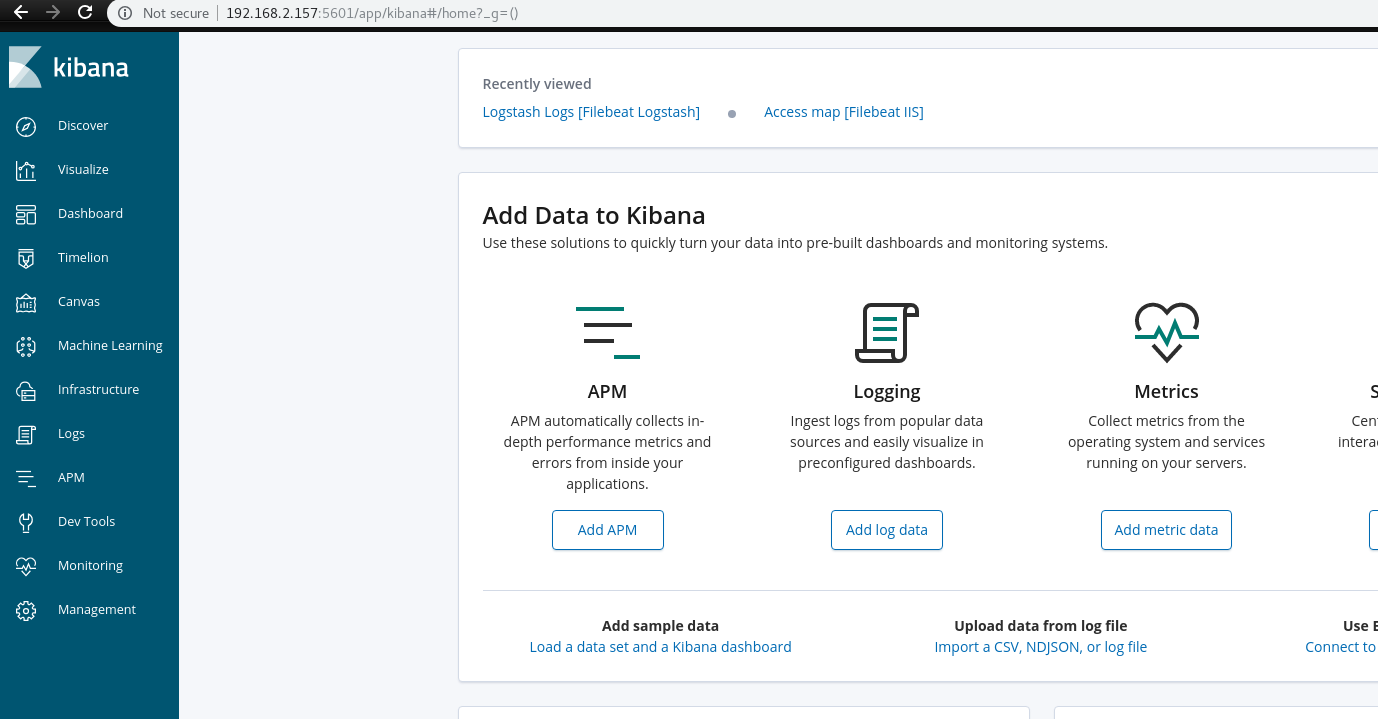
* **# vi /etc/kibana/kibana.yml**



Uncomment this three lines. As per image.

sudo systemctl start kibana

**Go to** browser and <http://your_server_ip:5601>



## 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

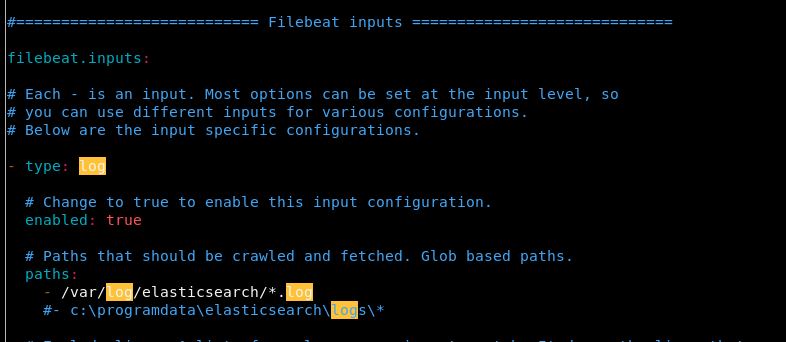
* # sudo systemctl enable logstash

## 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:**



#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

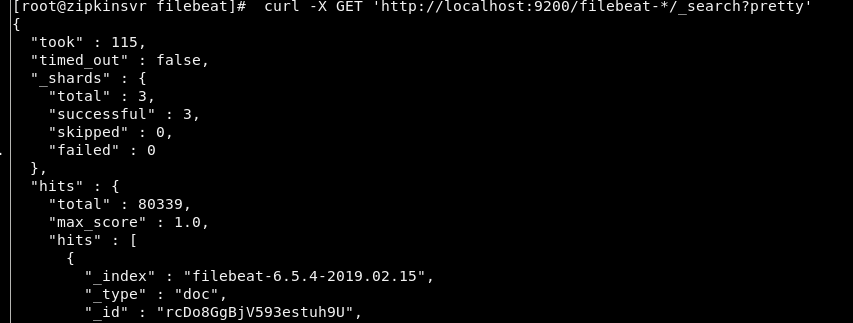
**Now start the filebeat**

* # 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:-

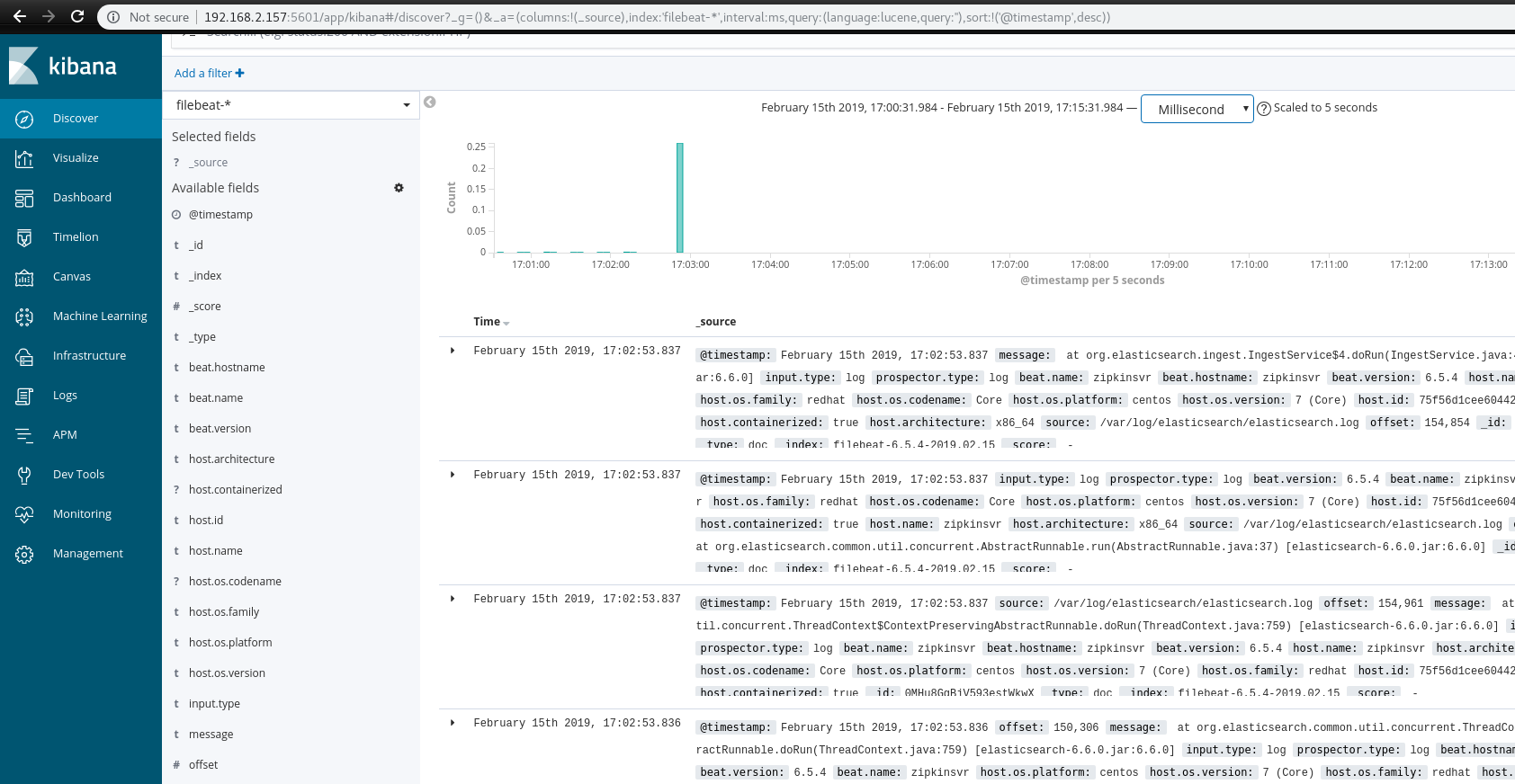


**Now Go to** KIbana Dashboard <http://localhost:5601/> OR IP:5601

Now click on **Discover**

Select **filebeat-\* index**

Then it will show logs as below:-



\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*