**EFK**

* Create a Ubuntu VM with 2 CPU s and 8 GB RAM in Azure with 22, 9200 and 5601 inbound ports open.
* Connect to VM using SSH by using following command

# ssh <user name>@<public IP address>

* Then you will be asked to enter password, Give the password and run following commands to install Elasticsearch, Kibana and Logstash (optional)

# apt-get update

**Install the Elastic Stack:**

* Import the Elasticsearch signing key and update your APT sources list to include the Elastic package repository by running following commands.

# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

# sudo apt -y install apt-transport-https

# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

# apt update

* Install the Java Virtual on the VM and configure the JAVA\_HOME variable-this is necessary for the Elastic Stack components to run.

# sudo apt update && sudo apt install openjdk-8-jre-headless export

# JAVA\_HOME=/usr/lib/jvm/java-8-openjdk-amd64

* Run the following commands to update Ubuntu package sources and install Elasticsearch, Kibana, and Logstash.

# sudo apt update && sudo apt install elasticsearch kibana

**Start Elasticsearch:**

* Start Elasticsearch on your VM with the following command:

# sudo systemctl start elasticsearch.service

* This command produces no output, so verify that Elasticsearch is running on the VM with this curl command:

# sudo curl 'localhost:9200/'

* If Elasticsearch is running, you see output like the following:

{

"name" : "w6Z4NwR",

"cluster\_name" : "elasticsearch",

"cluster\_uuid" : "SDzCajBoSK2EkXmHvJVaDQ",

"version" : {

"number" : "5.6.3",

"build\_hash" : "1a2f265",

"build\_date" : "2017-10-06T20:33:39.012Z",

"build\_snapshot" : false,

"lucene\_version" : "6.6.1"

},

"tagline" : "You Know, for Search"

}

## **Start Kibana and visualize the data in Elasticsearch:**

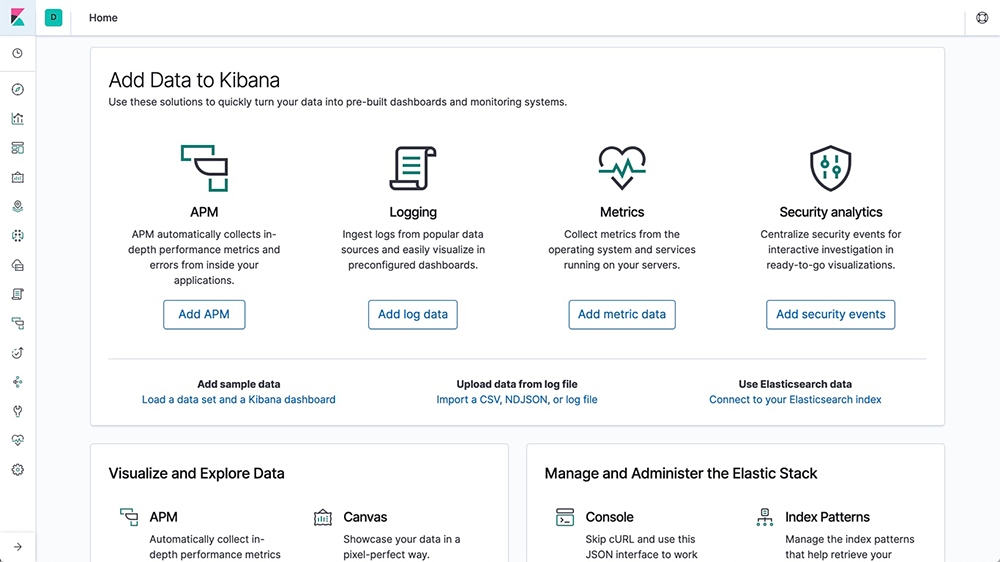
## Edit /etc/kibana/kibana.yml using vi/nano and change the IP address Kibana listens on so you can access it from your web browser.

server.host:"0.0.0.0”

* Start the Kibana server using following command:

sudo systemctl start kibana.service

* Open up the Kibana console with public ip address of VM along with 5601 port in your browser. Kibana will be redirected to page like this.



**Installing and configuring filebeat for logs:**

* Since we are using a Ubuntu VM, Filebeat can be downloaded and installed using below commands.

**- deb:**

# curl -L -O <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb>

# sudo dpkg -i filebeat-7.4.0-amd64.deb

* To configure the filebeat we have to edit Filebeat configuration file which is at /etc/filebeat/filebeat.yml. Open this configuration file using vi or nano
* Change the below lines in the configuration file with your values.

output.elasticsearch:

hosts: ["<es\_url>"]

setup.kibana:

host: "<kibana\_url>"

Dashboards:

setup.dashboards.enabled: true

Where <password> is the password of the elastic user, <es\_url> is the URL of Elasticsearch, and <kibana\_url> is the URL of Kibana.

* Once changes done, test the configuration using following commands.

# filebeat test config

# filebeat test output

* Filebeat has everything in terms of modules. We have to enable the module for which logs we want to forward to Kibana. Use the command to list all modules in filebeat.

# filebeat modules list

* To enable a particular module use below command.

# filebeat modules enable <module name>

Modify the settings in the /etc/filebeat/modules.d/<module name>.yml file if needed.

* The setup command loads the Kibana dashboards. And start filebeat using following commands.

# filebeat setup

# systemctl start filebeat

* Once the setup has been done we can check logs in the Kibana under discover section..

**Installing and configuring metricbeat for metrics:**

* Since we are using a Ubuntu VM, Filebeat can be downloaded and installed using below commands.

**- deb:**

# curl -L -O <https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.3.1-amd64.deb>

# sudo dpkg -i metricbeat-7.3.1-amd64.deb

* To configure the metricbeat we have to edit Filebeat configuration file which is at /etc/metricbeat/metricbeat.yml. Open this configuration file using vi or nano
* Change the below lines in the configuration file with your values.

output.elasticsearch:

hosts: ["<es\_url>"]

setup.kibana:

host: "<kibana\_url>"

Dashboards:

setup.dashboards.enabled: true

Where <password> is the password of the elastic user, <es\_url> is the URL of Elasticsearch, and <kibana\_url> is the URL of Kibana.

* Metricbeat has everything in terms of modules. We have to enable the module for which logs we want to forward to Kibana. Use the command to list all modules in metricbeat.

# metricbeat modules list

* To enable a particular module use below command.

# metrucbeat modules enable <module name>

Modify the settings in the /etc/metricbeat/modules.d/<module name>.yml file if needed.

* The setup command loads the Kibana dashboards. And start filebeat using following commands.

# metricbeat setup

# systemctl start metricbeat

* Once the setup has been done we can check metrics in the Kibana dashboard.