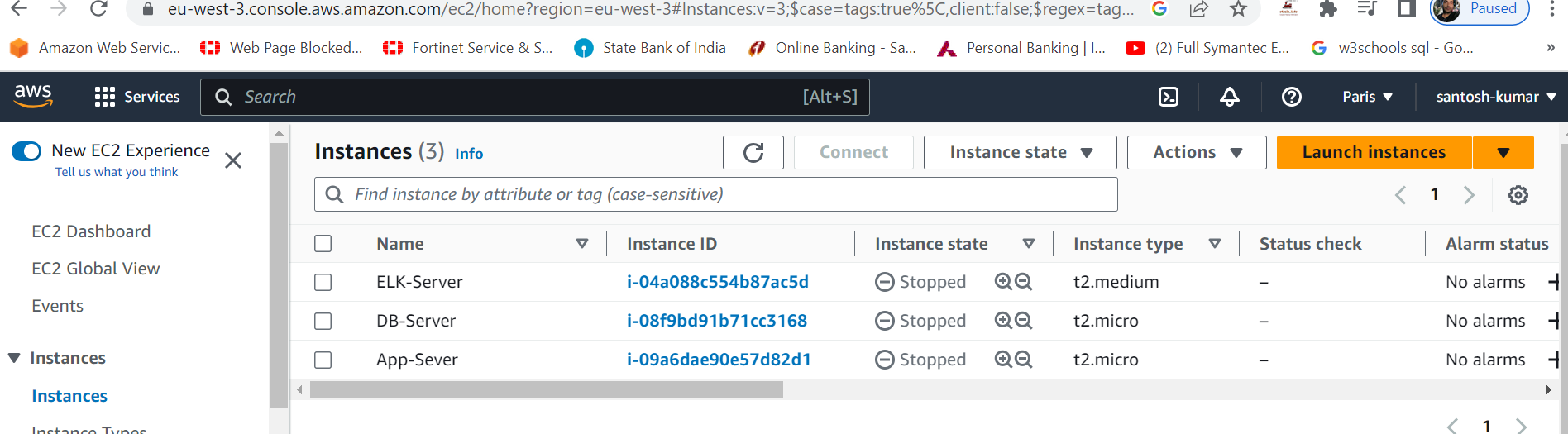
﻿

AWS Deployment

Deployed 3 EC2 instance on AWS cloud for ELK, App and database server.



Monitoring setup using ELK Stack

What is ELK?

Elastic Stack refers to a set of opensource products that have been developed by elastic to help it's users collect data from different types of sources and then analyze the collected data and represent it in an easy to understand and aesthetic visualization. This is done so that meaningful observations can be made.

Sources of Data - Elastic Stack - Visualizations

Components of ELK

* Elasticsearch - Elasticsearch is a NOSQL Database that was developed based on apache Lucene search engine. It can be used to index and store multiple different types of documents and data. It provides a function to search the data that is stored in real-time as it's being fed.

Used for storing & searching collected Data. ﻿

* Logstash -- Used for collecting & filtering the input data.Logstash is a collection agent and is used to collect both heterogenous/non-heterogenous data from various sources. It has the capability to screen, breakdown and make string alterations in the data it collects. After it has collected and filtered the data it then sends it to elastic search for storage.
* Kibana -- Provides a graphical user interface. ﻿Kibana is graphical user interface that is used to display the data that was collected and stored in Elasticsearch. It displays them with appealing visuals so that the data could be easily understood and analyzed, it does so using multiple different types of visuals like bar charts, pie chart, world maps, heat maps, co-ordinate maps etc.

Features of Kibana:

* Discover the data by exploring it.
* Analyze the data by applying different metrics.
* Visualize the data by creating different types of charts.
* Apply machine learning on ty data to get data anomaly
* Manage users and roles.
* A console to run Elasticsearch expressions.
* Play with time-series data using Timeline.
* Monitor elastic Stack using monitoring.
* Beats - Beats is similar to Logstash in the matter of fact that they both collect the data that will be later stored and analyzed, but beats differs in the method of collection.

Here beats are multiple small software installed on different servers from where they collect the data and send it to Elasticsearch.

ELK Flow﻿

* First the Beats are attached to remote servers from where the beats collect information from various sources.
* After collecting all the data needed they either ship the data to Logstash for filtration or directly send the data to Elasticsearch.
* The data is then stored in Elasticsearch, from here it will not be directly sent to Kibana. Kibana first needs to check where elasticsearch is and then go and get the data itself.

﻿Features of ELK

* System Performance Monitoring
* Log Management
* Application Performance Monitoring
* Application data analysis
* Security monitoring and alerting
* Data Vsualization

ELK Installation

﻿Pre-requisites:

1. At least 2GB of RAM 2. At least 20 GB storage 3. JAVA

- Installation Steps

-Launch EC2 instance on AWS

-Go to AWS console – Launch EC2 instance with Ubuntu server (here we are taking t2. medium)

﻿-Installing JAVA on the instance:

$ sudo apt-get update

$ sudo apt-get install -y openjdk-8-jdk

﻿

Installing nginx on the instance

$ sudo apt-get update

$ sudo apt-get -y install nginx

$ sudo systemctl enable nginx

﻿

Downloading and installing Elasticsearch:

$ wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.2.0-amd64.deb

$ sudo dpkg -i elasticsearch-7.2.0-amd64.deb

Downloading and installing kibana

﻿$ sudo wget <https://artifacts.elastic.co/downloads/kibana/kibana-7.2.0-amd64.deb>

$ sudo dpkg -i kibana-7.2.0-amd64.deb

Downloading and installing logstash

$ sudo apt-get install -y apt-transport-https

$ wget https://artifacts.elastic.co/downloads/logstash/logstash-7.2.0.deb

$ sudo dpkg -i logstash-7.2.0.deb

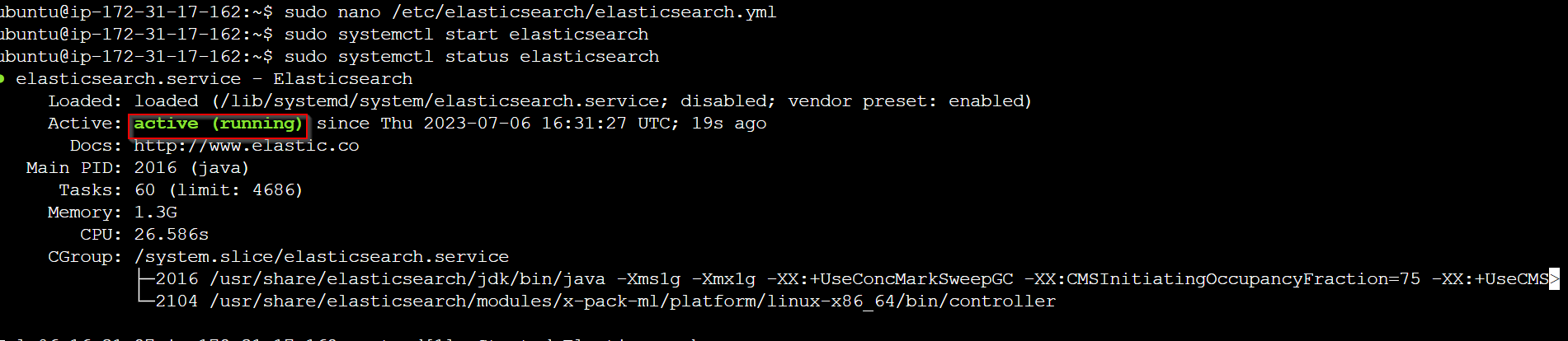
﻿Downloading and Installing Filebeat:

$ wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.2.0-amd64.deb

$ sudo dpkg -i filebeat-7.2.0-amd64.deb

Configuring Elastichsearch

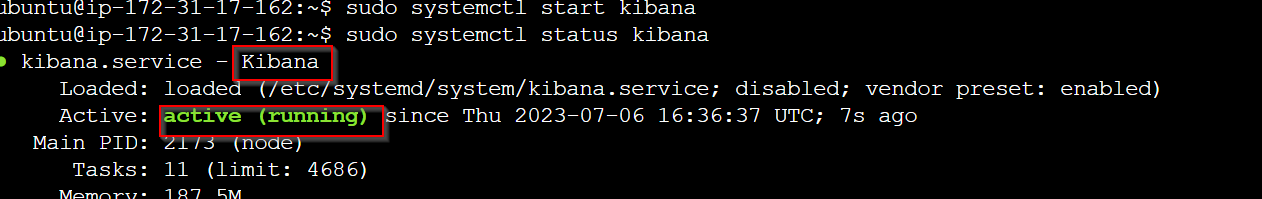
﻿sudo nano /etc/elasticsearch/elasticsearch.yml



﻿

Configuring Kibana

$ sudo nano /etc/kibana/kibana.yml



﻿$ sudo apt-get install -y apache2-utils

To create user and password for kibana console

﻿$ sudo htpasswd -c /etc/nginx/htpasswd.users kibadmin

User name kibadmin

Password kibadmin

To check the password

$ sudo nano /etc/nginx/htpasswd.users

﻿$ sudo nano /etc/nginx/sites-available/default – to connect nginx to kibana

Code to configure nginx to be connected to kibana

server {

listen 80;

server\_name <Instance Private IP>;

auth\_basic "Restricted Access";

auth\_basic\_user\_file /etc/nginx/htpasswd.users;

location / {

proxy\_pass http://localhost:5601;

proxy\_http\_version 1.1;

proxy\_set\_header Upgrade $http\_upgrade: proxy\_set\_header Connection 'upgrade'; proxy\_set\_header Host $host;

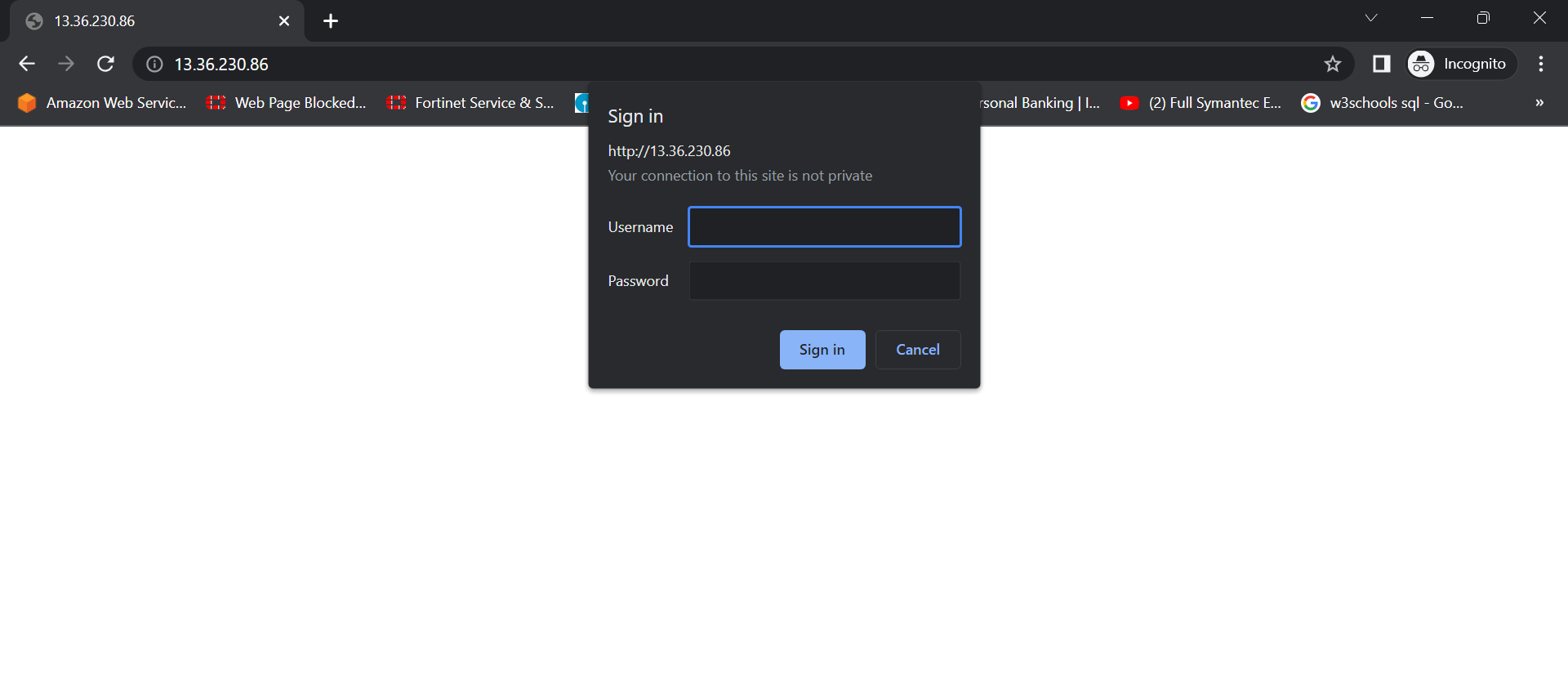
proxy\_cache\_bypass $http\_upgrade;

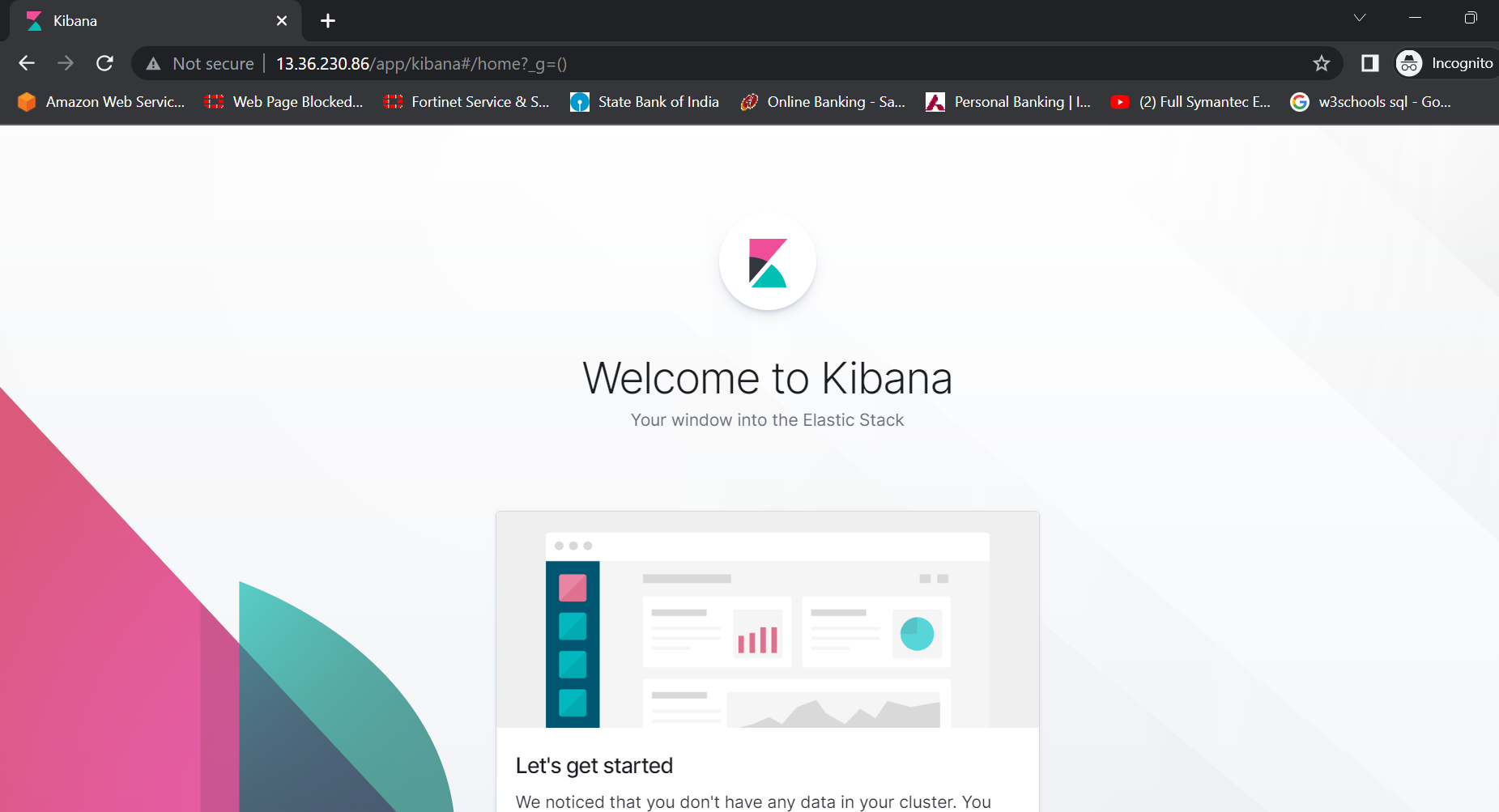
}

Start nginx

$ sudo systemctl start nginx

**Kibana is deployed in AWS cloud on UBUNTU server, and can be access from anywhere using browser**





﻿