Installing Elasticsearch

First, you need to add Elastic's signing key so that the downloaded package can be verified (skip this step if you've already installed packages from Elastic):

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

For Debian, we need to then install the apt-transport-https package:

sudo apt-get update
sudo apt-get install apt-transport-https

The next step is to add the repository definition to your system:

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

All that's left to do is to update your repositories and install Elasticsearch:

sudo apt-get update
sudo apt-get install elasticsearch

Elasticsearch configurations are done using a configuration file that allows you to configure general settings (e.g. node name), as well as network settings (e.g. host and port), where data is stored, memory, log files, and more.

For our example, since we are installing Elasticsearch on AWS, it is a good best practice to bind Elasticsearch to either a private IP or localhost:

sudo vim /etc/elasticsearch/elasticsearch.yml

network.host: "localhost"
http.port:9200
cluster.initial_master_nodes: ["<PrivateIP"]

To run Elasticsearch, use:

sudo service elasticsearch start

Installing Logstash

Logstash requires Java 8 or Java 11 to run so we will start the process of setting up Logstash with:

sudo apt-get install default-jre

Verify java is installed:

java -version

openjdk version "1.8.0_191"
OpenJDK Runtime Environment (build 1.8.0_191-8u191-b12-2ubuntu0.16.04.1-b12)
OpenJDK 64-Bit Server VM (build 25.191-b12, mixed mode)

Since we already defined the repository in the system, all we have to do to install Logstash is run:

sudo apt-get install logstash

Before you run Logstash, you will need to configure a data pipeline. We will get back to that once we've installed and started Kibana.

Install Kibana

As before, we will use a simple apt command to install Kibana:

sudo apt-get install kibana

Open up the Kibana configuration file at: */etc/kibana/kibana.yml*, and make sure you have the following configurations defined:

server.port: 5601
elasticsearch.url: "http://localhost:9200"

These specific configurations tell Kibana which Elasticsearch to connect to and which port to use.

Now, start Kibana with:

sudo service kibana start

Open up Kibana in your browser with: http://localhost:5601. You will be presented with the Kibana home page.