**Interview Questions**

**What is ELK**

ELK can securely pull and analyze and visualize the data in real-time from any source and formate

**Elasticsearch**

It is a distributed search, analytic engine at the heart of the ELK stack

* It provides near real-time search and analytics for all types of data
* We can store data in ES

**Logstash**

It is a plugin-based data collector and processing engine

* It is a lightweight, open-source, and server-side data collector pipeline
* It allows to collect data from a variety of sources & send it to the desired destination

**Kibana**

Kibana is a visualization tool

* It is a free and open user interface
* It visualizes our ES data & navigate the ELK stack

**What is an Elasticsearch cluster?**

The collection of connected nodes is known as a cluster, a cluster can also consist of a single node.

**What is an Elasticsearch Index?**

An index is a logical namespace that points to one or more shards and replicas in an ES cluster

**What does the term document mean in Elasticsearch?**

Documents are JSON objects that are distributed across your Elasticsearch cluster which are accessible from any node.

**What are the advantages of using Logstash?**

* Over 200 plugins available
* Process unstructured data
* Pre-built and custom filters
* Built custom data processing pipelines

**What are the advantages of using Kibana?**

* Real-time observability
* Integration with Elasticsearch
* Browser-based visualization tool
* It is a free and open user interface
* It is a visualization of our ES data & navigates the elastic stack

**How do you check the version of Elasticsearch you are working with?**

Execute the curl command from our command line:

curl -XGET '[http://localhost:9200](http://localhost:9200/)'

**How do you create an index in Elasticsearch?**

Use the following command to create a new Elasticsearch index:

PUT /my-index-000001

**How do you load data into Elasticsearch?**

To get started with loading data into Elasticsearch you will ideally want to use one of the many available Beats to load data into Logstash for further processing within Elasticsearch. Popular Beats include the following:

[Filebeat](https://logit.io/sources/configure/filebeat), [Metricbeat](https://logit.io/sources/configure/metricbeat), [Heartbeat](https://logit.io/sources/configure/heartbeat), [Auditbeat](https://logit.io/sources/configure/auditbeat), [Packetbeat](https://logit.io/sources/configure/packetbeat)

**Where does Elasticsearch store data?**

For Debian/Unbuntu this will be located at /var/lib/elasticsearch/data

For RHEL/CentOS this will be located at /var/lib/elasticsearch

**How do you check if Elasticsearch is running?**

curl -XGET <http://localhost:9200/_status>

**How do you stop Elasticsearch (how to kill the process)**

PS -ef | grep Elasticsearch

Kill -9 process ID

**What database does Elasticsearch use?**

Elasticsearch is a NoSQL database

**What is the curl command?**

The curl command in Elasticsearch allows you to take many actions including but not limited to: deleting indexes, list all indexes, list all documents within an index, query using URL parameters, add data and list index mappings.

**How do you delete an index in Elasticsearch?**

By using the DELETE /index name. Command.

**How can you test Logstash performance?**

You can use the [**node stats API**](https://www.elastic.co/guide/en/logstash/current/node-stats-api.html) to retrieve runtime statistics from Logstash.

**Where are Kibana dashboards stored?**

Kibana dashboards are stored in Elasticsearch under the default **index kibana-int** which can be edited within the config.js file if you wish to store your dashboards in a different location.

**What is Grok?**

Grok is a filter plugin for Logstash that is used to parse unstructured data. It is often used for transforming Apache, Syslog and other webserver logs into a structured and queryable format for easier data analysis to be performed.

**List out the different operations that can be performed on the document using an Elasticsearch?**

1. Indexing 2) Updating 3) Fetching 4) Deleting

**Can you list X-Pack commands?**

1. Migrate 2) Users 3) Syskeygen 4) Setup-passwords 4) Certgen

**What is the syntax or code to retrieve a document by ID in Elasticsearch?**

GET <index\_name>/\_doc/<\_id>

**Where is Elastic search stored?**

Elastic search results are stored in a distributed document in different directories. Also, a user can retrieve complex data structures that are serialized as JSON documents.

**What is the syntax or code to add a Mapping in an Index🡪** POST /\_<index\_name>/\_type/\_id

**Elasticsearch shell script**

#!/bin/bash

es-status= curl -XGET <http://hostname> -f :9200/-cat/health -k -s -u elastic | cut -c20-43

echo “$es-status”

if [ $es-status == ‘green’ ]

then

echo “elasticsearch is running”

else

echo “elasticsearch is down” send mail -f [kalva.kumar@gmail.com](mailto:kalva.kumar@gmail.com) -t [pavanasri@gmail.com](mailto:pavanasri@gmail.com)

/data/elasticsearch-8.1.0/bin/elasticsearch &

fi

**Kibana shell script**

**#!/bin/bash**

**Var= $(curl -XGET –user elasticsearch : vv5….** [**http://Kibana**](http://Kibana) **IP:5601/status -I | head -n 1 | cut -c10-12)**

**Echo “$var”**

**If [ $var = ‘200’ ]**

**Then**

**Echo “kibana is runing”**

**Else**

**Kill $(lsof -t -i:5601)**

**Sleep 5**

**Echo “kibana is down” send mail -f kalva.kumar@gmail.com -t** [**pavanasri@gmail.com**](mailto:pavanasri@gmail.com)

**/data/kibana-8.1.0/bin/kibana &**

**Crontab -e**

**\*/5 \* \* \* \* file -zcpf path**

**Netstat -tulpn | grep port ==> check the running port**