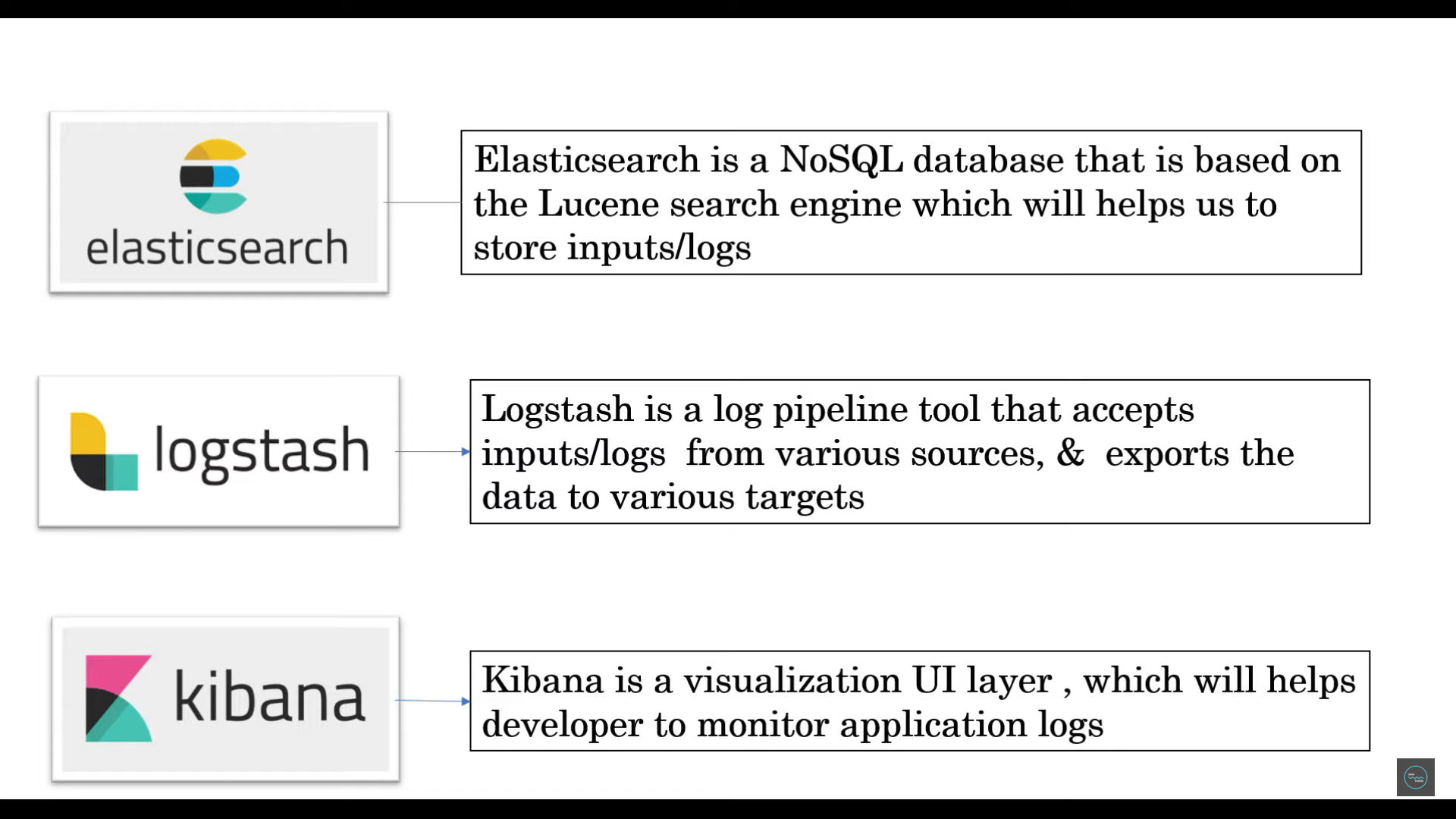
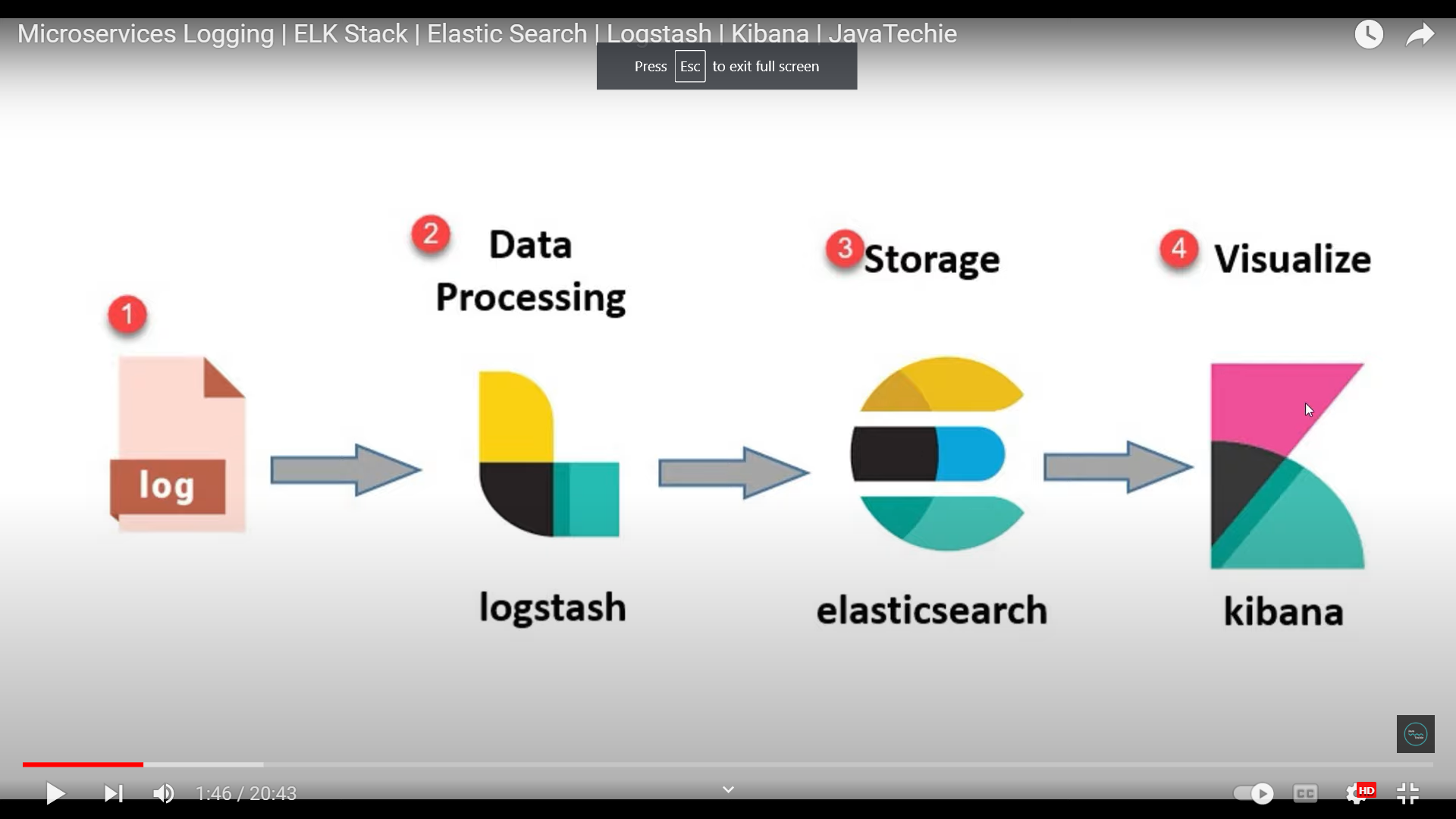
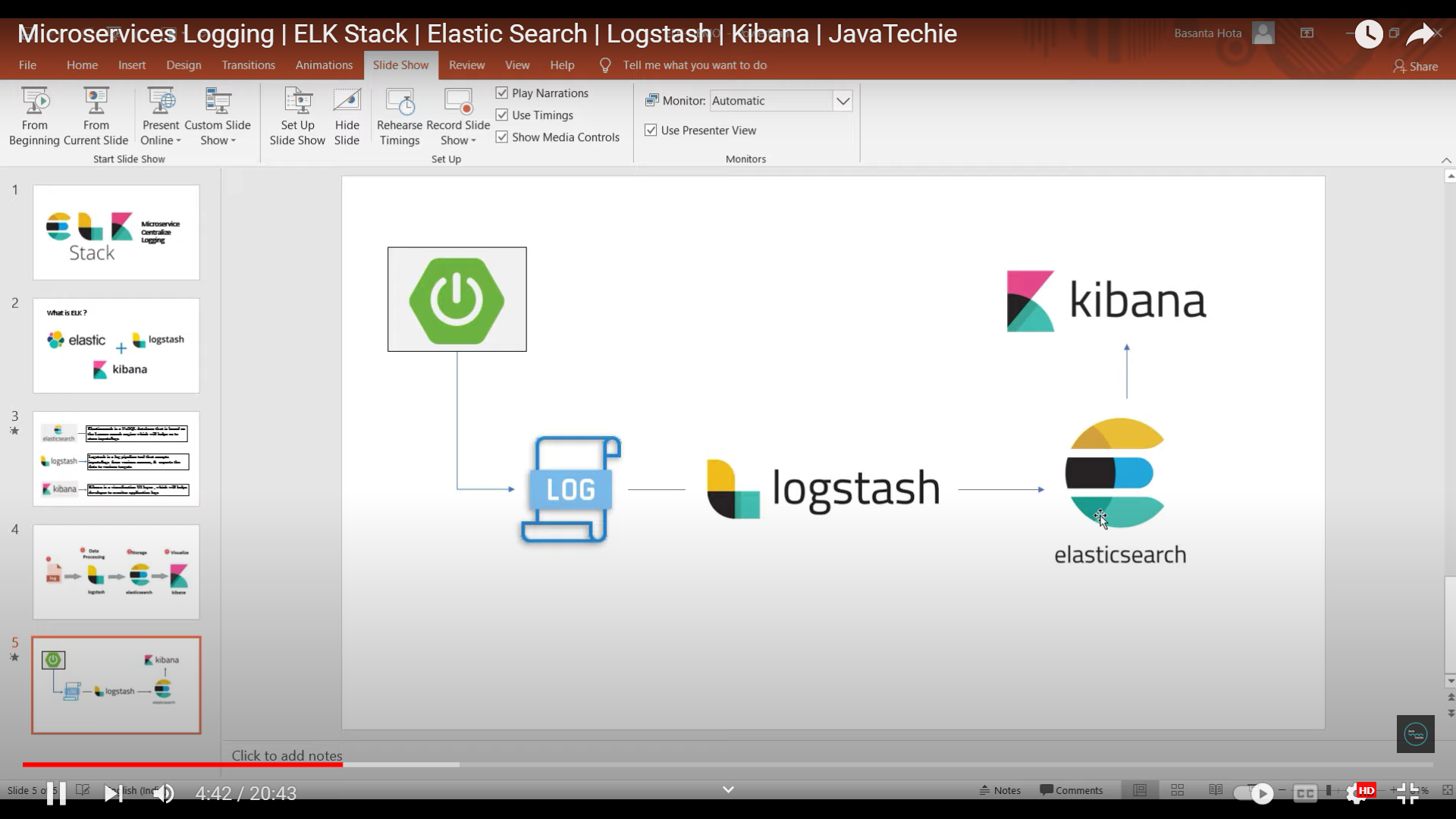
https://www.youtube.com/watch?v=5s9pR9UUtAU&ab\_channel=JavaTechie

ELK is used for centralized Loging mechanism.



Elastic Search is internally using NoSql DB.





To check the elasticsearch is up and running or not we can hit the url = http://localhost:9200/

Configure username and password for elastic search below.

<https://www.youtube.com/watch?v=nhlwEf5AZf0&ab_channel=SoumilShah>

<https://www.elastic.co/guide/en/elasticsearch/reference/current/users-command.html#_examples_13>

step-1

Disable the ssl for elasticsearch.yml file below

xpack.security.http.ssl:

  enabled: false

xpack.security.transport.ssl:

  enabled: false

Step -2

For new elastic search there is no user and password exist. So we need to create the user and password and what is the role of that particular user that can be configured in below command.

Bin folder/ elasticsearch-users useradd khagendra -p khagendrapwd -r network,monitoring,admins

Now check the users and users\_roles file in the elastic search config folder. The user and roles are added to the file to access the elasticsearch.

Step -3

Add the below roles to to roles.yml file

admins:

  cluster:

    - all

  indices:

    - names:

        - "\*"

      privileges:

        - all

devs:

  cluster:

    - manage

  indices:

    - names:

        - "\*"

      privileges:

        - write

        - delete

        - create\_index

Step – 3

To check the elasticsearch is up and running or not we can hit the url = <http://localhost:9200/>

And pass the username and password.

Connecting ElasticSearch with Kibana

<https://www.youtube.com/watch?v=BybAetckH88&ab_channel=SoumilShah>

<https://github.com/soumilshah1995/learning-logstash-and-elastic-search-plugins/blob/main/ELKStack8.3/readme.md>

Step – 1

Add below configuration in elasticsearch.yml file to reset and show the password

action.auto\_create\_index: .monitoring\*,.watches,.triggered\_watches,.watcher-history\*,.ml\*

Step – 2

Start the elastisearch.bat file to up and run the elastic search server.

Step -3

Open new cmd for elastic search and run the below command for user elastic and kibana\_system user and note down the password.

elasticsearch-reset-password -u elastic

elasticsearch-reset-password -u kibana\_system

NOTE THE PASS ON NOTEPAD

Step -4

Now modify the kibana.yml file by uncommenting the below configuration

server.port: 5601

server.host: "localhost"

elasticsearch.hosts: ["http://localhost:9200"]

elasticsearch.username: "kibana\_system"

elasticsearch.password: "<put the reset password for kibana\_system from step 3>"

Step - 5

Now start the kibana.bat file to start the Kibana server.

Step -6

Hit the url = <http://localhost:5601/>

Give the username = elastic

Give the password = <put the reset password for elastic user from step3>

Configuration of logstash with Elastic search, Kibana

<https://www.youtube.com/watch?v=BybAetckH88&ab_channel=SoumilShah>

Step -1

ElasticSearch and Kibana should be up and running.

Step -2

Go inside logstash >> config folder and modify the logstash-sample.conf file below



input {

stdin {

}

}

output {

stdout {

codec => rubydebug

}

elasticsearch {

hosts => ["http://localhost:9200"]

index => "test.logstash"

user => "elastic"

password => ""<put the reset password for elastic user from step 3>"

}

}

Step -3

Start the logstash sever by below command.

logstash -f .\config\logstash-sample.conf --config.reload.automatic

logstash -f .\config\logstash.conf --config.reload.automatic

after successfully start the server give some user input from the server console log below

>> hello khagendra

>> hello i m first user

Step -4

Go to kibana url = <http://localhost:5601/>

Then Management >> Dev Tools >> console

The create the indices as follow PUT test.logstash

Then get the details use this command = GET test.logstash/\_search

