**INSTALLATION GUIDE FOR ELK**

**1: install java jdk**

sudo yum install java-1.8.0-openjdk

**2: Import the elk pgp-key**

sudo rpm ––import https://artifacts.elastic.co/GPG-KEY-elasticsearch

**3: Add repo for elk**

cd /etc/yum.repos.d/

sudo vim elasticsearch.repo

**Add this in file**

[elasticstack]

name=Elastic repository for 7.x packages

baseurl=https://artifacts.elastic.co/packages/7.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

**4: install elk**

sudo yum -y install elasticsearch kibana logstash

**5: now configure your elasticsearch**

**ADD ENTERY IN HOST FILE**

**Vim /etc/hosts**

vi /etc/elasticsearch/elasticsearch.yml

discovery.type: single-node

**uncomment the network.host and port**

#network.host: localhost

#port:9200

Add this in end

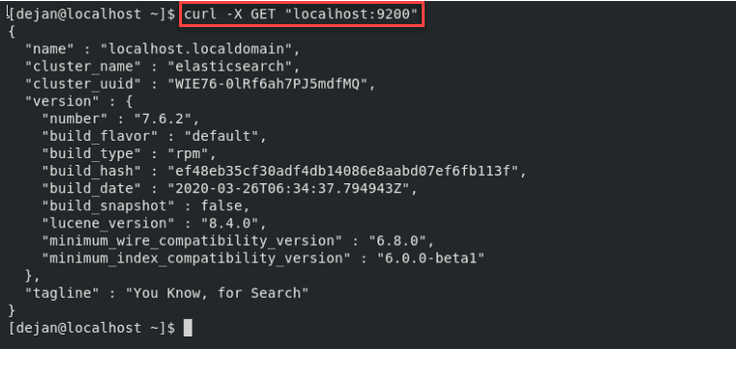
i

START THE ELASTICSEARCH

systemctl start elasticsearch

TEST YOUR CONNECTION

curl -X GET "localhost:9200"



**5: now configure kibana**

**UNCOMMENT ALL OF THESE**

#server.host: "localhost"

#port=5601

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

Start kibana

sudo systemctl start kibana

**6: check your browser**

<http://localhost:5601>

**7: configure logstash**

[**https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-centos-7**](https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-centos-7)

**use upper link for configure logstash filebeat**