**Elasticsearch**

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

go to sudo vi /etc/elasticserch/elasticsearch.yml

add

network.host: 127.0.0.1

http.host: 0.0.0.0

server.port: 9200

sudo yum install elasticsearch

go to sudo vi /etc/elasticsearch/elasticsearch.yml

network.host: localhost

sudo systemctl start elasticsearch

sudo systemctl enable elasticsearch

curl -X GET "localhost:9200"

Output

{

"name" : "8oSCBFJ",

"cluster\_name" : "elasticsearch",

"cluster\_uuid" : "1Nf9ZymBQaOWKpMRBfisog",

"version" : {

"number" : "6.5.2",

"build\_flavor" : "default",

"build\_type" : "rpm",

"build\_hash" : "9434bed",

"build\_date" : "2018-11-29T23:58:20.891072Z",

"build\_snapshot" : false,

"lucene\_version" : "7.5.0",

"minimum\_wire\_compatibility\_version" : "5.6.0",

"minimum\_index\_compatibility\_version" : "5.0.0"

},

"tagline" : "You Know, for Search"

}

**KIBANA**

sudo yum install kibana

sudo systemctl enable kibana

sudo systemctl start kibana

sudo nano /etc/kibana/kibana.yml

server.host: 0.0.0.0

server.port: 5601

curl -X GET "localhost:5601"

**Filebeat**

Download and install the public signing key:

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

Create a file with a .repo extension (for example, elastic.repo) in your /etc/yum.repos.d/ directory and add the following lines:

[elastic-8.x]

name=Elastic repository for 8.x packages

baseurl=https://artifacts.elastic.co/packages/8.x/yum

gpgcheck=1

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

enabled=1

autorefresh=1

type=rpm-md

sudo yum install filebeat

sudo nano /etc/filebeat/filebeat.yml

output.elastic:

hosts: [“localhost:9200”]

http.host: 0.0.0.0

server.port: 9200