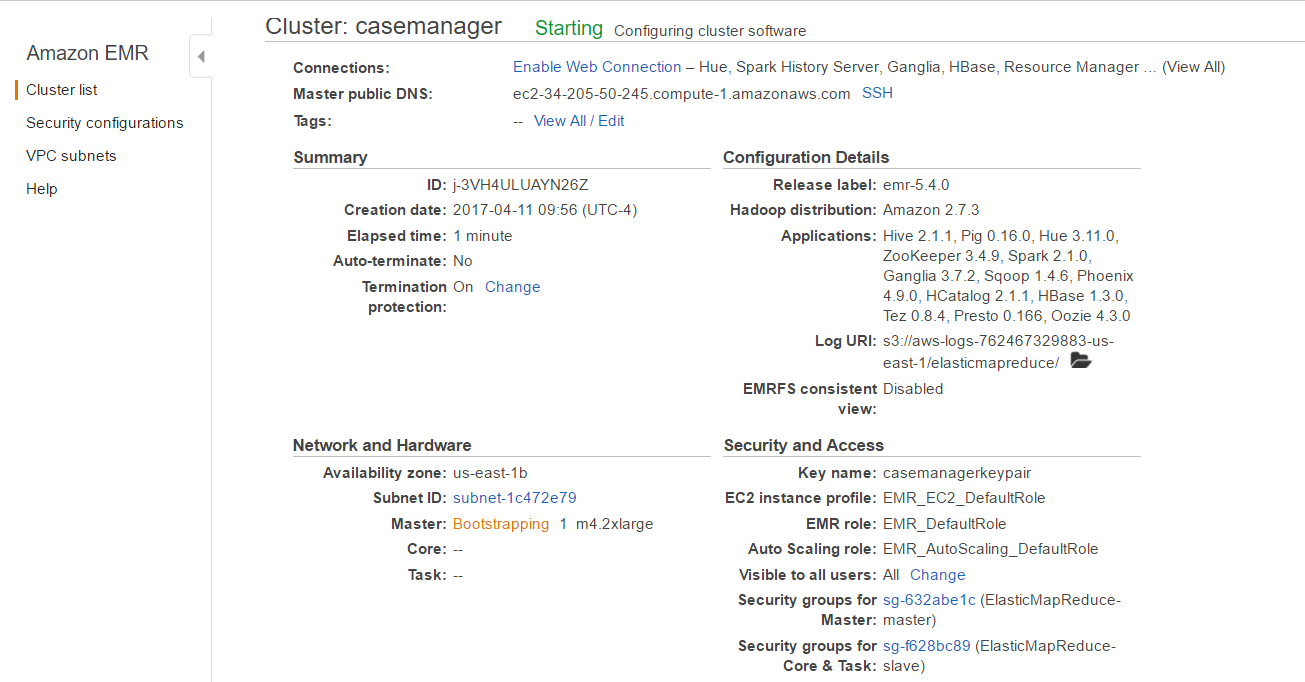
Create an EMR Cluster with Hadoop,Hive & Spark



Create an elastic ip and associate it with the ec2 instance –ip which is running

****

**How to connect to putty**

Login to 34.197.207.249 using putty.

Use the casemanagerkeypair.ppk as private key in auth tab in putty.

Username is Hadoop

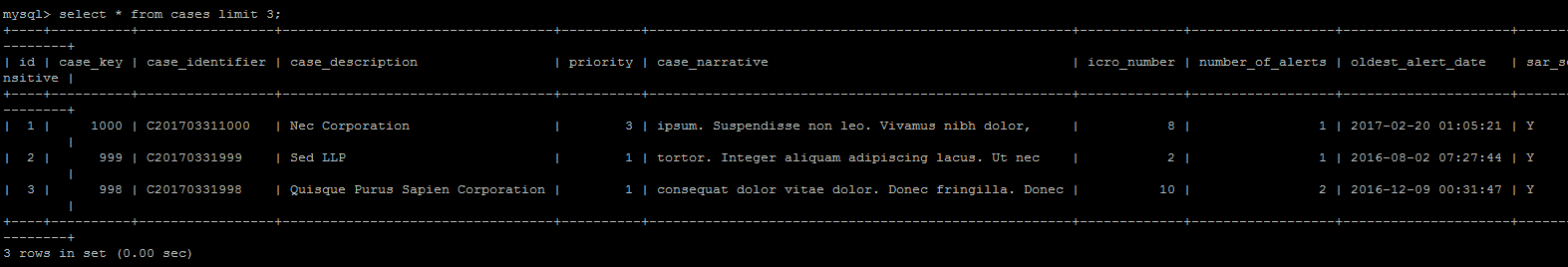
Open mysql

Use casemanager;

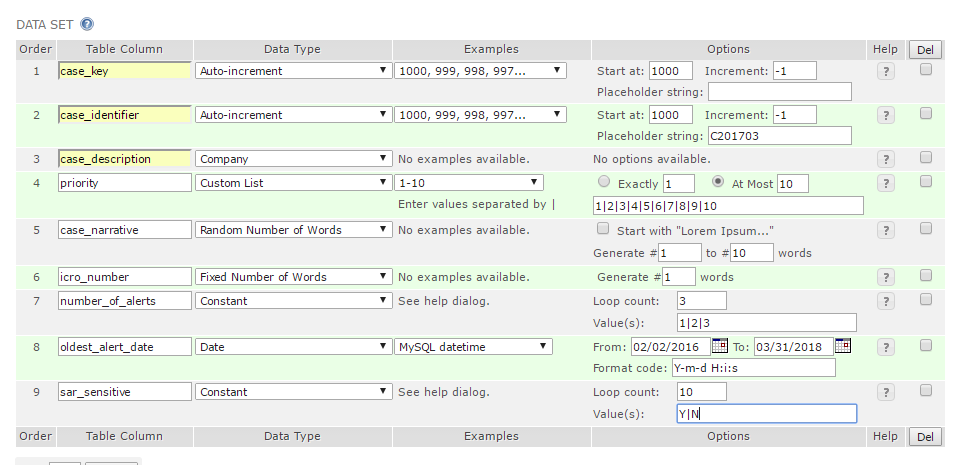
Select \* from cases;

*Generate the data using*

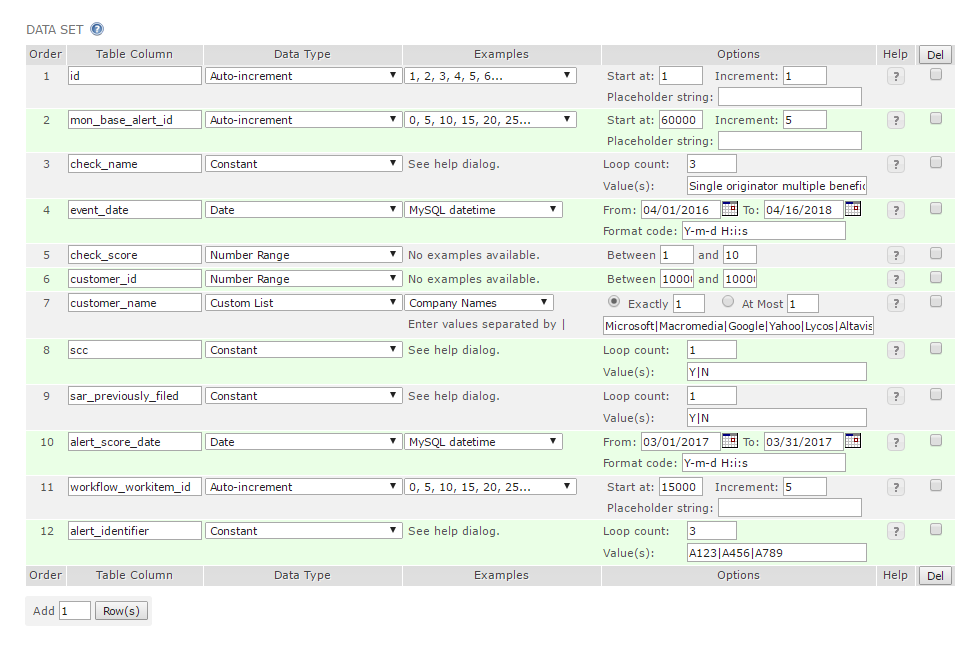
*Inserted the data*



*Sample testdata generator tool*



**Sample testdata for mon\_alert**



**Instructions for creating the elasticsearch cluster.**

sudo rpm -i <https://download.elastic.co/elasticsearch/release/org/elasticsearch/distribution/rpm/elasticsearch/2.3.3/elasticsearch-2.3.3.rpm>

sudo chkconfig --add elasticsearch

Open "/etc/elasticsearch/elasticsearch.yml" on every machine and edit the following settings.

*cluster.name:esonaws bootstrap.mlockall: true*

*discovery.zen.ping.unicast.hosts: “private ip address of ec2 instance”*

*network.host:”private ip address of ec2 instance”*

Start the service 🡪 sudo service elasticsearch start

Check the status of elastic search service 🡪

curl 34.197.207.249:9200/\_cluster/health?pretty

**Instructions for install of kibana.**

Download the Kibana 4.4.2 version

Gunzip gile.zip

Tar –xvf file.tar

Update kibana.yml file in config folder with below changes

elasticsearch.url: <http://34.197.207.249:9200>

server.host: "172.31.12.199" (private ip )

start kibana as ./bin/kibana

open kibana ui - <http://34.197.207.249:5601>