**Steps:**

1. Traverse ‘<elasticsearch path>’ and copy below files/folders to the ‘/tmp/elk\_home/’ directory of respective data nodes –

bin

config

1. Traverse ‘<elasticsearch path>/elasticsearch-7.7.0/’ and copy below files/folders to the ‘/tmp/elk\_home/’ directory of respective data nodes -

securityadmin\_demo.sh

1. Traverse ‘<elasticsearch path>/elasticsearch-7.7.0/config/’ and copy below files/folders to the ‘/tmp/elk\_config/’ directory of respective data nodes -

roles.yml

role\_mapping.yml

log4j2.properties

certs

root-ca.pem

kirk.pem

kirk-key.pem

esnode.pem

esnode-key.pem

elasticsearch.keystore

users\_roles

users

jvm.options

elasticsearch.yml

1. Traverse ‘<elasticsearch path>/elasticsearch-7.7.0/plugins’ and copy below files/folders to the ‘/tmp/elk\_plugins/’ directory of respective data nodes -

opendistro-job-scheduler

opendistro\_security

opendistro\_alerting

1. Use below mentioned commands to add the data node –

cd <elasticsearch path>

sudo -u gmedia tar -xzf /tmp/elasticsearch-7.7.0-linux-x86\_64.tar.gz

sudo -u gmedia cp -r /tmp/elk\_home/\* ./

cd <elasticsearch path>/elasticsearch-7.7.0/config/

sudo -u gmedia cp -r /tmp/elk\_config/\* ./

cd <elasticsearch path>/elasticsearch-7.7.0/plugins

sudo -u gmedia cp -r /tmp/elk\_plugins/\* ./

cd /DATA/

sudo -u gmedia mkdir elk

sudo -u gmedia mkdir elk/elasticsearch

sudo -u gmedia mkdir elk/elasticsearch/data

cd <elasticsearch path>/config

update data folder path in elasticsearch.yml file

cd <elasticsearch path>/bin

Update the elasticsearch home path in es-data.sh file

sudo -u gmedia ./es-data.sh start

sudo -u gmedia ./securityadmin\_demo.sh