**OpenDistro Plugins Installation: -**

1. Download Opendistro “Job Scheduler and Alerting plugins” from below link (strictly follow version compatibility) and copy it to /tmp/ directory in every node of Elasticsearch and Kibana server.

<https://opendistro.github.io/for-elasticsearch-docs/docs/install/plugins/>

Download link for version 1.8 :-

Elasticsearch plugins: -

<https://d3g5vo6xdbdb9a.cloudfront.net/downloads/elasticsearch-plugins/opendistro-job-scheduler/opendistro-job-scheduler-1.8.0.0.zip>

<https://d3g5vo6xdbdb9a.cloudfront.net/downloads/elasticsearch-plugins/opendistro-alerting/opendistro_alerting-1.8.0.0.zip>

<https://d3g5vo6xdbdb9a.cloudfront.net/tarball/opendistro-elasticsearch/opendistroforelasticsearch-1.8.0.tar.gz>

Kibana Plugins: -

<https://d3g5vo6xdbdb9a.cloudfront.net/downloads/kibana-plugins/opendistro-alerting/opendistro-alerting-1.8.0.0.zip>

<https://d3g5vo6xdbdb9a.cloudfront.net/downloads/opendistro-kibana/opendistroforelasticsearch-kibana-1.8.0.tar.gz>

1. Execute below commands to install the plugins –

**Elasticsearch Plugins Installation**

*Job-Scheduler plugins: -*

<elasticsearch home path>/bin/elasticsearch-plugin install <file:///tmp/Elasticsearch-opendistro-job-scheduler-1.8.0.0.zip>

*Alerting plugins: -*

<elasticsearch home path>/bin/elasticsearch-plugin install <file:///tmp/Elasticsearch-opendistro_alerting-1.8.0.0.zip>

**Kibana Plugins Installation: -**

*Alerting plugins: -*

<kibana home path>/bin/kibana-plugin install file:///tmp/ kibana-opendistro-alerting-1.8.0.0

1. Use below commands to unzip the files –

sudo -u gmedia tar -xzf /tmp/opendistroforelasticsearch-1.8.0.tar.gz

sudo -u gmedia tar -xzf /tmp/opendistroforelasticsearch-kibana-1.8.0.tar.gz

1. Update Kibana.yml using below commands –

sudo -u gmedia vi <kibana home path>/config/kibana.yml

Update with below text –

opendistro\_security.multitenancy.enabled: true

opendistro\_security.multitenancy.tenants.preferred: ["Private", "Global"]

opendistro\_security.readonly\_mode.roles: ["kibana\_read\_only"]

newsfeed.enabled: false

telemetry.optIn: false

telemetry.enabled: false

Copy the kibana plugins to location using below commands –

sudo -u gmedia cp -r /tmp/opendistroforelasticsearch-kibana/plugins/opendistro\_security <kibana home path>/plugins/

Update elasticsearch.yml using below commands –

sudo -u gmedia vi <elasticsearch home path>/config/elasticsearch.yml

Update with below text –

######## Start OpenDistro for Elasticsearch Security Demo Configuration ########

# WARNING: revise all the lines below before you go into production

opendistro\_security.ssl.transport.pemcert\_filepath: esnode.pem

opendistro\_security.ssl.transport.pemkey\_filepath: esnode-key.pem

opendistro\_security.ssl.transport.pemtrustedcas\_filepath: root-ca.pem

opendistro\_security.ssl.transport.enforce\_hostname\_verification: false

opendistro\_security.ssl.http.enabled: false

opendistro\_security.ssl.http.pemcert\_filepath: esnode.pem

opendistro\_security.ssl.http.pemkey\_filepath: esnode-key.pem

opendistro\_security.ssl.http.pemtrustedcas\_filepath: root-ca.pem

opendistro\_security.allow\_unsafe\_democertificates: true

opendistro\_security.allow\_default\_init\_securityindex: true

opendistro\_security.authcz.admin\_dn:

- CN=kirk,OU=client,O=client,L=test, C=de

opendistro\_security.audit.type: internal\_elasticsearch

opendistro\_security.enable\_snapshot\_restore\_privilege: true

opendistro\_security.check\_snapshot\_restore\_write\_privileges: true

opendistro\_security.restapi.roles\_enabled: ["all\_access", "security\_rest\_api\_access"]

cluster.routing.allocation.disk.threshold\_enabled: false

node.max\_local\_storage\_nodes: 3

######## End OpenDistro for Elasticsearch Security Demo Configuration ########

1. Use below commands on all Kibana nodes to copy the plugins –

sudo -u gmedia cp -r /tmp/opendistroforelasticsearch-kibana/plugins/opendistro\_security <kibana home path>/plugins/

1. Use below commands on all elasticsearch nodes to copy the plugins –

sudo -u gmedia cp -r /tmp/opendistroforelasticsearch-1.8.0/plugins/opendistro\_security <elasticsearch home path>/plugins/

1. Run below commands to install the configuration –

cd <elasticsearch home path>/plugins/opendistro\_security/tools/

sudo -u gmedia sh install\_demo\_configuration.sh

1. Copy the created keystore, certificate files to all the elasticsearch nodes.
2. Restart elasticsearch nodes.
3. Run the below command to create the users in elasticsearch in all nodes –

sudo -u gmedia sh securityadmin\_demo.sh

1. Restart Kibana nodes.