ELK stack Notes:

1. URLs:

Elastic search:

\*\*\*\*\*\*\*\*\*\*\*\*

<http://indevl-elasti01.dtc.dish.corp:9200/>

<http://indevl-elasti02.dtc.dish.corp:9200/>

Kibana:

\*\*\*\*\*\*\*

<http://indevl-kibana01.dtc.dish.corp:5601/app/kibana#/home?_g=()>

1. Elastic Search Config Changes:

When you do any change to the configuration (even a URL), the default security check will be enforced (as it will treat as PROD instead of Dev) and simple warnings such as boot strap check, VM max sixe etc…will cause the server to be shutdown.

To prevent this:

sudo sysctl -w vm.max\_map\_count=262144

Or you can add permanently in /etc/sysctl.conf:

grep vm.max\_map\_count /etc/sysctl.conf

vm.max\_map\_count=262144

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

If you want to use hostname:<port> as a URL, you have to change the below configuration in “elasticsearch.yml”

# ---------------------------------- Network -----------------------------------

#

# Set the bind address to a specific IP (IPv4 or IPv6):

#

network.host: 0.0.0.0

#

# Set a custom port for HTTP:

#

http.port: 9200

#

# For more information, consult the network module documentation.

Run Elastic search as deamon use “./bin/elasticsearch -d -p pid”

systemctl status elasticsearch

systemctl start elasticsearch

1. KafKa Settings:

We must start Zookeeper instance before starting Kafka. So please use the below commands for the same. Zookeeper start script will use zookeeper.properties file as an input.

./zookeeper-server-start.sh ../config/zookeeper.properties

Kafka instance will use server.properties file as an input like below:

./kafka-server-start.sh ../config/server.properties &

./kafka-reassign-partitions.sh --zookeeper inprdl-kafka01.dtc.dish.corp:2181 --reassignment-json-file /apps/software/kafka\_2.11-2.0.0/increase-replication-factor.json --execute

1. Kibana:

Please do the following changes in kibana.yml file under configurations. We have server elastic search URL as an input so that Kibana instance will try to ping every second and retrieve the result/content.

# Kibana is served by a back end server. This setting specifies the port to use.

server.port: 5601

# To allow connections from remote users, set this parameter to a non-loopback address.

server.host: "indevl-kibana01.dtc.dish.corp"

# The URL of the Elasticsearch instance to use for all your queries.

elasticsearch.url: "http://indevl-elasti01.dtc.dish.corp:9200/"

Issues:

There will be a Master Node and a Data node in the cluster known as “Report-Dashboard” in our environment.

After initial set up Elasticsearch Node1 as Master and Node2 as Data, we have faced couple of issues like Shards are not available, this is because of actual node is converted as master, so cluster ignoring the data in its data folder.

This is because we have not inserted any data in second Node and we have converted first node to Master Node.

We have resolved this by setting first node as Master & Data (so that It will consume the contents from Node1) and we have added second node as a Data Node.

Cluster configuration is complete in Elastic Search.