**US ELASTICSEARCH UPDATE ACTIVITY**

**POINTS TO BE DONE ON THIS ACTIVITY**

* **Stop Alerts from BOT-PROD-App1 & DB Server**
* **Supervisor service stop from BOT-PROD-App1**
* **Take ES Configuration file Backup**
* **Take a ES backup from prod DB Server: 172.31.0.30**
* **Purge & Installation of Elasticsearch 7.8 on Prod DB Server 172.31.0.30**
* **Adding Local & ES Snapshot repo Path**
* **Restart supervisorctl on BOT-PROD-App1**
* **Start Alerts from BOT-PROD-App1 & DB Servers**

**NOTE: Before doing activity need to stop Alerts from Server.**

1. **Stop Cronjob on BOT-PROD-App1 & DB Server**

* **DB Server Cronjob – Need to be Stop**

#DB Alert

\*/1 \* \* \* \* sh /script/monitor\_script/service\_check.sh >>/dev/null 2>&1

0 0 \* \* \* sh /script/db-backup/elasticsearch\_backup.sh >>/dev/null 2>&1

* **App Server Cronjob – Need to be Stop**

Comment supervisor cron

1. **Stop Supervisor Service**

**RUN ON APP-1**

systemctl stop supervisorctl

1. **Elasticsearch Conf directory Backup on DB Server**

Copy configuration file /etc/elasticsearch

1. **Take a ES backup from prod DB Server: 172.31.0.30**

**ES S3 & Local Dump on DB Server**

sh /script/db-backup/elasticsearch\_backup\_local.sh -> Local Backup  
sh /script/db-backup/elasticsearch\_backup.sh -> S3 Backup

bucket location : surbo-prod-dbbackup/Elasticsearch

* **Take Snapshot name from below location**

**log\_file=/var/log/backups/es\_snapshot.log**

<<<<<<<---------------Taking Snapshot of cluster-------------------->>>>>>>>>

====>>>>Taking snapshot of elasticsearch named: **snapshot\_25012021-000001**  
====>>>>Time@Snapshot is started:000001  
====>>>>Total time taken for snapshotting:  
====>>>>snapshot:snapshot\_25012021-000001 status:completed  
<<<<<<<<<---------------End of snapshotting--------------------->>>>>>>>>>>

1. **Purge Elasticsearch on DB Server:**

apt purge elasticsearch

rm –rf /var/lib/elasticsearch /var/log/elasticsearch /etc/elasticsearch/

**Remove data from data directory**

mv /elasticseacrhData/es-backup /elasticseacrhData/es-backup\_3feb2021  
mkdir /elasticseacrhData/es-backup  
chown –R elasticsearch.elasticsearch /elasticseacrhData/es-backup

**ES Installation**

**NOTE: Before installation check compatible JDK version installed or not. For 7.8 we need JDK 11.08 which we have on server. IF not updated JDK then update Java.**

1. **JAVA Installation 11.09**

sudo apt-get update

sudo apt-get install openjdk-11-jdk-headless

java -version

1. **Elasticsearch 7.8 Installation**  
   **Import the Elasticsearch PGP Key**

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

### Installing from the APT repository

sudo apt-get install apt-transport-https

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

**You can install the Elasticsearch Debian package with:**

sudo apt-get update &&

For Stable

sudo apt-get install elasticsearch

For Specific Version

sudo apt-get install elasticsearch=7.8.0

**Elasticsearch can be started and stopped using the service command:**

sudo -i service elasticsearch start

sudo -i service elasticsearch stop

### Running Elasticsearch with systemd

sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable elasticsearch.service

sudo systemctl start elasticsearch.service

sudo systemctl stop elasticsearch.service

### Checking that Elasticsearch is running

curl -X GET "172.31.0.30:9200/?pretty"

**Update local IP on elasticsearch.yml file**

vi /etc/elasticsearch/elasticsearch.yml

path.data: /var/lib/elasticsearch  
path.logs: /var/log/elasticsearch  
  
network.host: 172.31.0.30  
  
**then add below lines**  
**discovery.type: single-node**

path.repo: ["/elasticseacrhData/es-backup"]

**Allowing Insecure settings**

**Default 2g**

-Xms4g

-Xmx4g

**Add the below line:  -Des.allow\_insecure\_settings=true It is working for me. there is an undocumented system property**  
 **cd /etc/elasticsearch/jvm.options**  
-Des.allow\_insecure\_settings=true

systemctl restart elasticsearch

1. **Adding Local BACKUP PATH**

curl -XPUT -H "Content-Type: application/json;charset=UTF-8" 'http://172.31.0.30:9200/\_snapshot/esbackup' -d '{ "type": "fs", "settings": { "location": "/elasticseacrhData/es-backup", "compress": true }}'

curl -X PUT "172.31.0.30:9200/\_snapshot/s3\_repository?pretty" -H 'Content-Type: application/json' -d'{"type": "s3","settings": {"bucket" : "surbo-prod-dbbackup","region" : "us-east-1", "base\_path" : "Elasticsearch7.8","access\_key":"ABCDEFGHIJKLMNO","secret\_key":"GeMK5LkK4H3kZu8Tn+niszqraeuNB/d3qr/mBblW"}}'

**NOTE: Update ACCESS\_KEY & SECRET\_KEY**

1. **Restart Supervisor Service on APP1**

**Run on App-1**

systemctl restart supervisorctl

1. **Start Cron Services from ALL DB & APP Servers.**