**ELASTICSEARCH UPDATE ACTIVITY**

**POINTS TO BE DONE ON THIS ACTIVITY**

* **Stop Alerts from App & DB Server**
* **Take a ES backup from prod DB Server: 10.1.26.67**
* **Restore ES backup on APP Server: 10.1.26.66**
* **Cross check Indices on both side**
* **Purge & Installation of Elasticsearch 7.8 on Prod DB Server 10.1.26.67**
* **Adding Local Snapshot repo Path**
* **Restart supervisorctl on App1**
* **Start Alerts from App & DB Server**

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

1. **Stop Alert from Cronjob on App & DB Server**

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

\*/1 \* \* \* \* sh /script/monitor\_scripts/service\_check.sh >> /script/monitor\_scripts/logs/monitor\_script\_`\/bin\/date +\%Y\%m\%d`.log

###Elastic search backup#####

0 0 \* \* \* sh /script/db-backup/elasticsearch\_backup.sh >> /script/db-backup/logs/es\_backup.log

#script for db check

\*/1 \* \* \* \* sh /script/monitor\_scripts/supervisor\_monitor.sh uae-prod-db1 >> /script/monitor\_scripts/logs/db\_`\/bin\/date +\%Y\%m\%d`.log

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

#502 alert

\* \* \* \* \* sh /script/monitor\_script/monitor\_502.sh dashboard >>/dev/null 2>&1

\* \* \* \* \* sh /script/monitor\_script/monitor\_502.sh chatbot >>/dev/null 2>&1

#supervisorcheck

\*/1 \* \* \* \* sh /script/monitor\_script/supervisor\_monitor.sh Middle-East-1 https://bothealth.surbo.io >> /var/log/monitor\_log/monitor\_script.log

1. **Take a ES backup from prod DB Server: 10.1.26.67**

**ES Local Dump on DB Server**

update s3 repository snapshot name in script and run

* **ES Local Dump on DB Server**

sh /script/db-backup/elasticsearch\_backup.sh

* **Take Snapshot name from below location**

**log\_file=/script/db-backup/logs/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. **Restore ES backup on APP Server: 10.1.26.66**

* **Copy Data Directory from DB to App Server**

scp –r –P 2291 sunny@10.1.26.67: /elasticseacrhData/es-backup/ /tmp

cp –r /tmp /elasticseacrhData/es-backup/

chown –R elasticsearch.elasticsearch /elasticseacrhData/es-backup/

* **ES Restore on App Server**

curl -XPOST <http://10.1.26.66:9200/_snapshot/esbackup/snapshot_???????????/_restore>

1. **Cross check Data/Indices from below command on both side**

curl 10.1.26.66:9200/\_cat/indices - APP SERVER

curl 10.1.26.67:9200/\_cat/indices - DB SERVER

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\_25jan2021  
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 "10.1.26.67:9200/?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: 172.31.87.199  
  
**then add below lines**  
**discovery.type: single-node**path.repo: ["/elasticseacrhData/es-backup"

**Allowing Insecure settings**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://10.1.26.66:9200/\_snapshot/esbackup' -d '{ "type": "fs", "settings": { "location": "/elasticseacrhData/es-backup", "compress": true }}'

1. **Restart Supervisor Service on APP1**

Systemctl restart supervisorctl

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