**Elasticsearch Backup & Restoration Process:**

In order to take backup of elasticsearch one network directory needs to be mounted. It can be shared with NFS or Samba .

Create a directory where we have to keep the snapshot

Example:

mkdir /opt/esbackup

Provide group ownership of elasticsearch to the directory

Chown :elasticsearch /opt/backup

Now use the below command to set the directory as a snapshot dir

Open /etc/elasticsearch/elasticsearch.yml

Path.repo: /opt/es-backup

Execute the below command to

curl -X PUT "10.100.76.90:9200/\_snapshot/my\_backup" -H 'Content-Type: application/json' -d'{"type": "fs","settings": {"location": "/opt/es-backup","compress": true}}'

Command to check snapshot :

curl -X GET "l0.100.76.90:9200/\_snapshot/es\_backup/\_status"

Use below REST api to take the backup:

PUT /\_snapshot/my\_backup/bcp?wait\_for\_completion=true

{

"indices":".kibana"

}

How to restore:

curl -X POST "10.100.76.90:9200/\_snapshot/es\_backup/bcp/\_restore?pretty"

How to check all snapshots available in elasticsearch:

GET /\_cat/snapshots/my\_backup

GET /\_cat/snapshots/my\_backup?v

How to verify Backup for cluster.

curl -XPOST 'http://10.100.76.90:9200/\_snapshot/my\_backup/\_verify'

How to get snapshot id :

GET /\_snapshot/my\_backup/\_all?pretty

One example for restoration:

curl -X POST "10.100.76.90:9200/\_snapshot/my\_backup/filebeat.20180912-104654/\_restore?pretty"

In case you are trying to restore on the same Cluster ,Index needs to be close first.

curl -X POST "10.100.76.90:9200/filebeat\*/\_close"

curl -X POST "10.100.76.90:9200/filebeat\*/\_open"

If the index needs to be restored with a different name below is the command:

POST /\_snapshot/my\_backup/\_restore

{

"indices": "filebeat",

"ignore\_unavailable": "true",

"include\_global\_state": false,

"rename\_pattern": "filebeat1",

"rename\_replacement": "filebeat1"

}

Points to remember:

To restore on a different cluster first of all we need to register the directory where we have all the snapshot. Curl commands are given above for this .

Script to create snapshot daily.



Script to delete the old snapshots.



Script to create tar file:



More scripts.



SAMBA Related commands:

Smbclient //10.100.76.90/ES-BACKUP -U elasticsearch

mount -t cifs //10.100.76.90/ES-BACKUP -o username=elasticsearch /opt/es-backup

mount -t cifs //10.100.76.90/ES-BACKUP -o username=elasticsearch /opt/es-backup/

The below entry needs to be made in /etc/fstab file

//10.100.76.90/ES-BACKUP /opt/es-backup cifs username=elasticsearch,password=\*\*\*\* 0 0