Q. how to recover deleted index in Elasticsearch?

Refer: https://www.udemy.com/course/elasticsearch-and-elastic-stack-in-depth-and-hands-on/learn/lecture/7276298

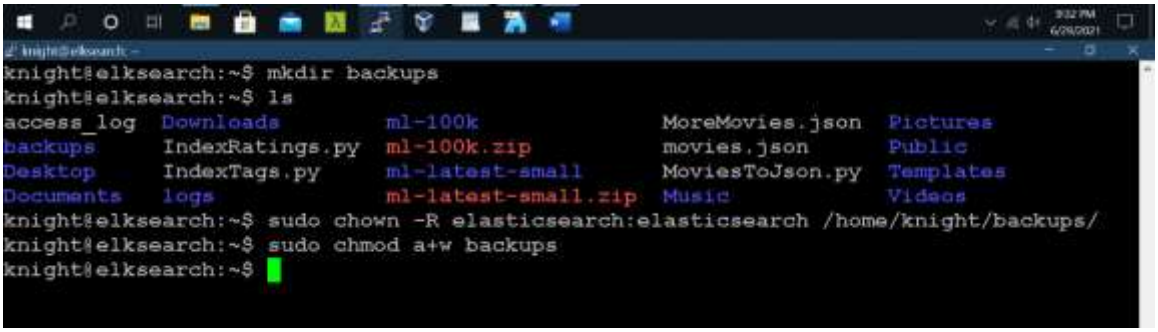
Step 1: Make backup directory on local machine i.e., /home/knight/backups

$mkdir backups

Step 2: Give permissions to write in that directory.

$ sudo chown -R elasticsearch:elasticsearch /home/knight/backups/

$sudo chmod a+w backups

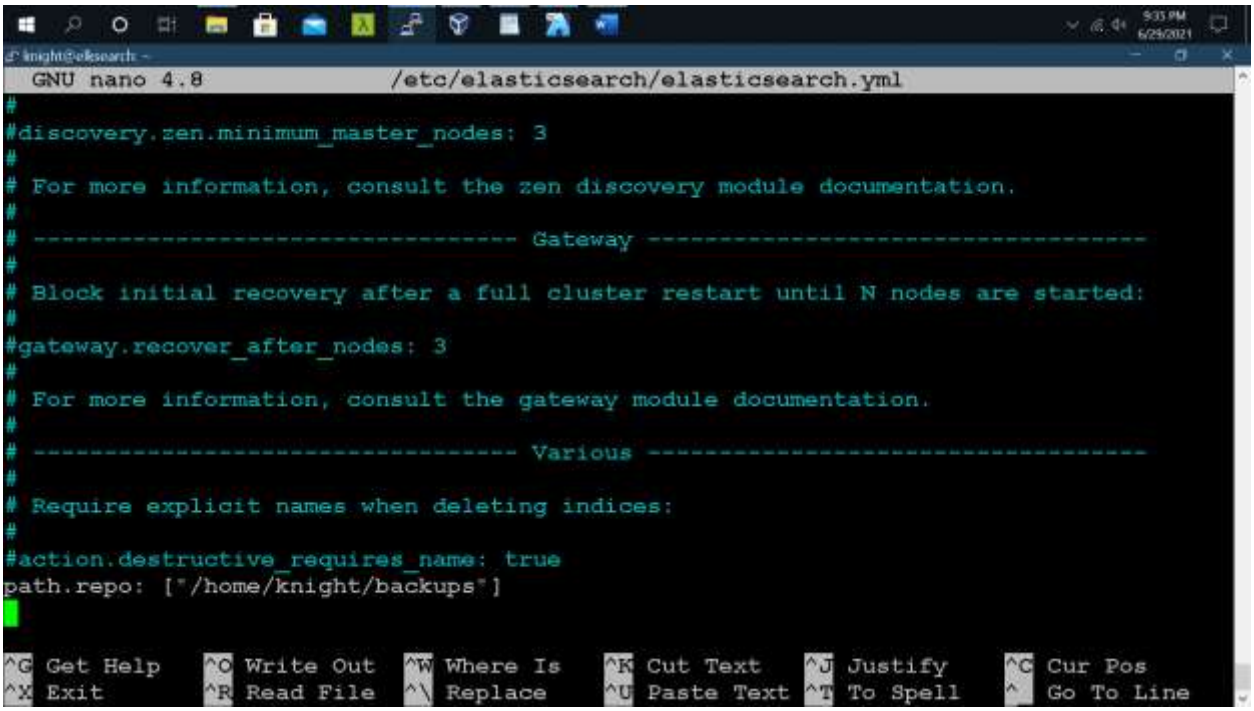


Step 3: Make entry in the .yml file of elasticsearch i.e., /etc/elasticsearch/elasticsearch.yml

$ sudo nano /etc/elasticsearch/elasticsearch.yml

Add following line at the end of the yml file and save,

path.repo: ["/home/knight/backups"]

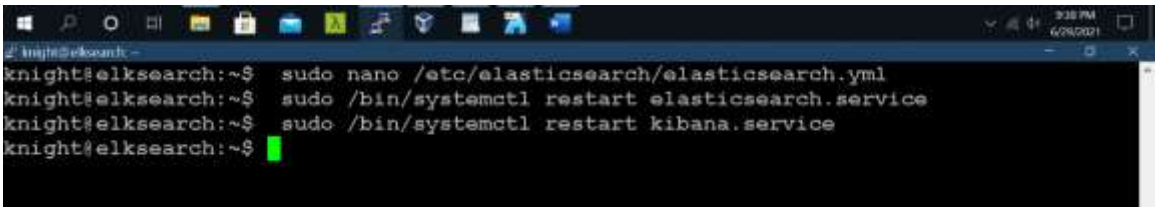


Step 4: Restart the elasticsearch service

$ sudo /bin/systemctl restart elasticsearch.service

Step 5: restart kibana

$ sudo /bin/systemctl restart kibana.service

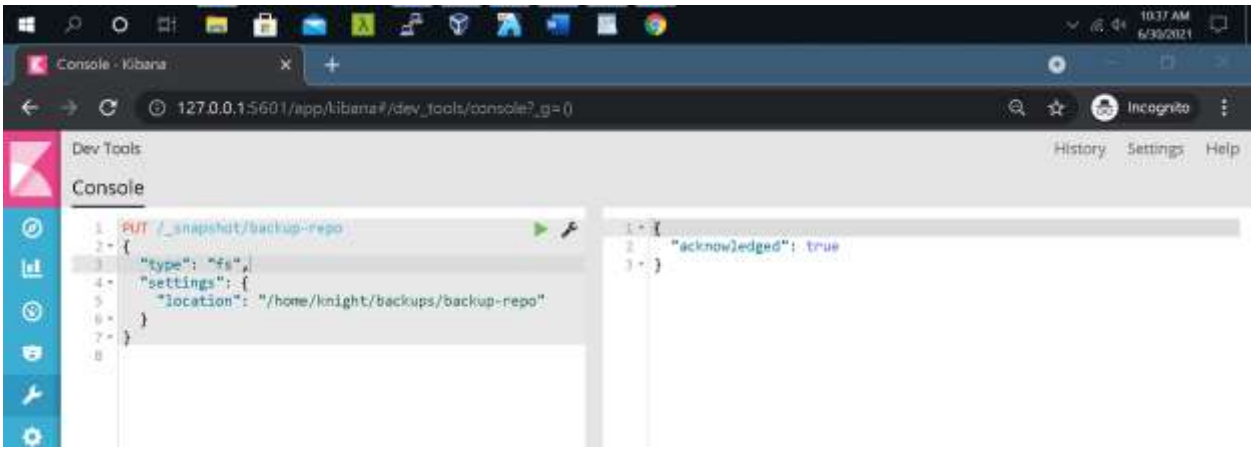


Step 6: Now go to browser and open kibana – 127.0.0.1:5601 and open DevTool

Step 7: Register a snapshot repository before you can perform snapshot and restore operations.

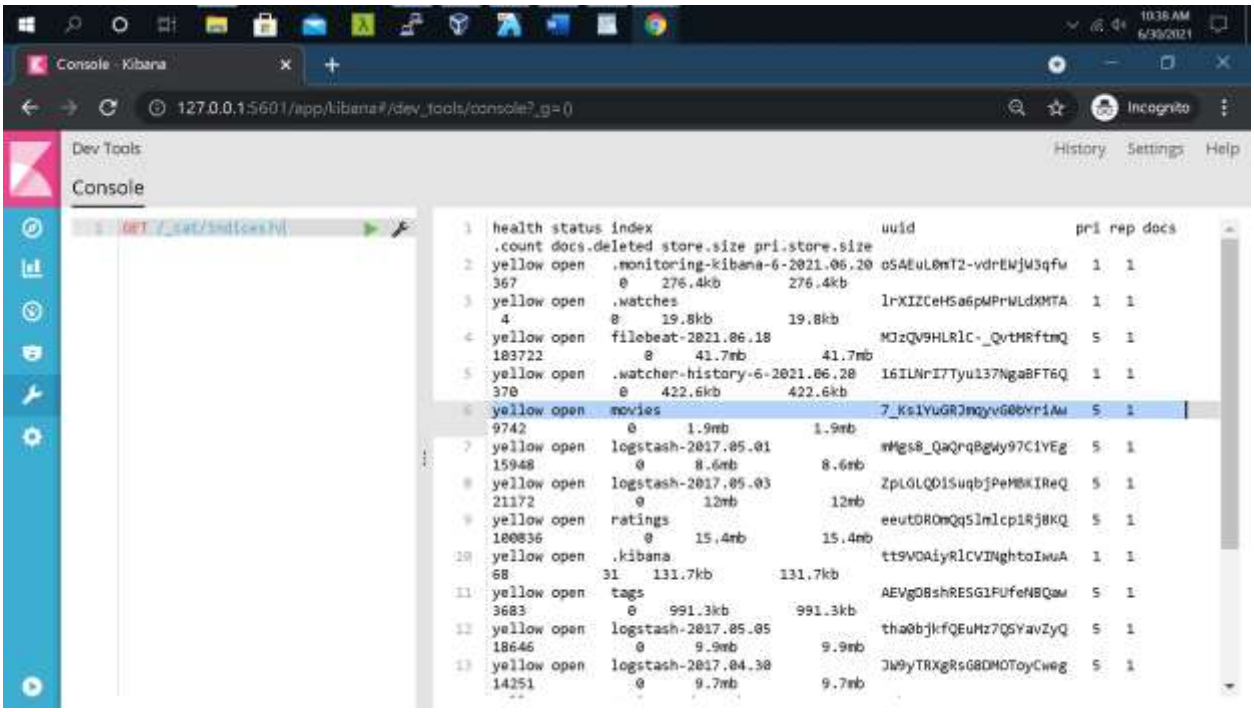
```
>>>PUT /_snapshot/backup-repo
{
  "type": "fs",
  "settings": {
```

```
  "location": "/home/knight/backup/backup-repo"
 }
}
```



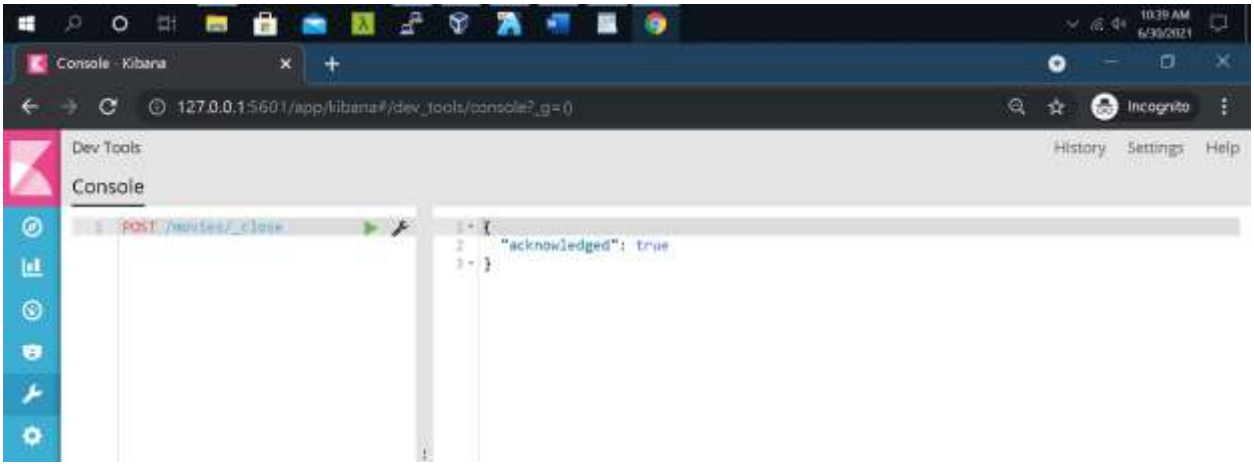
Step 8: View all indices present in ES database

>>>GET /_cat/indices?v

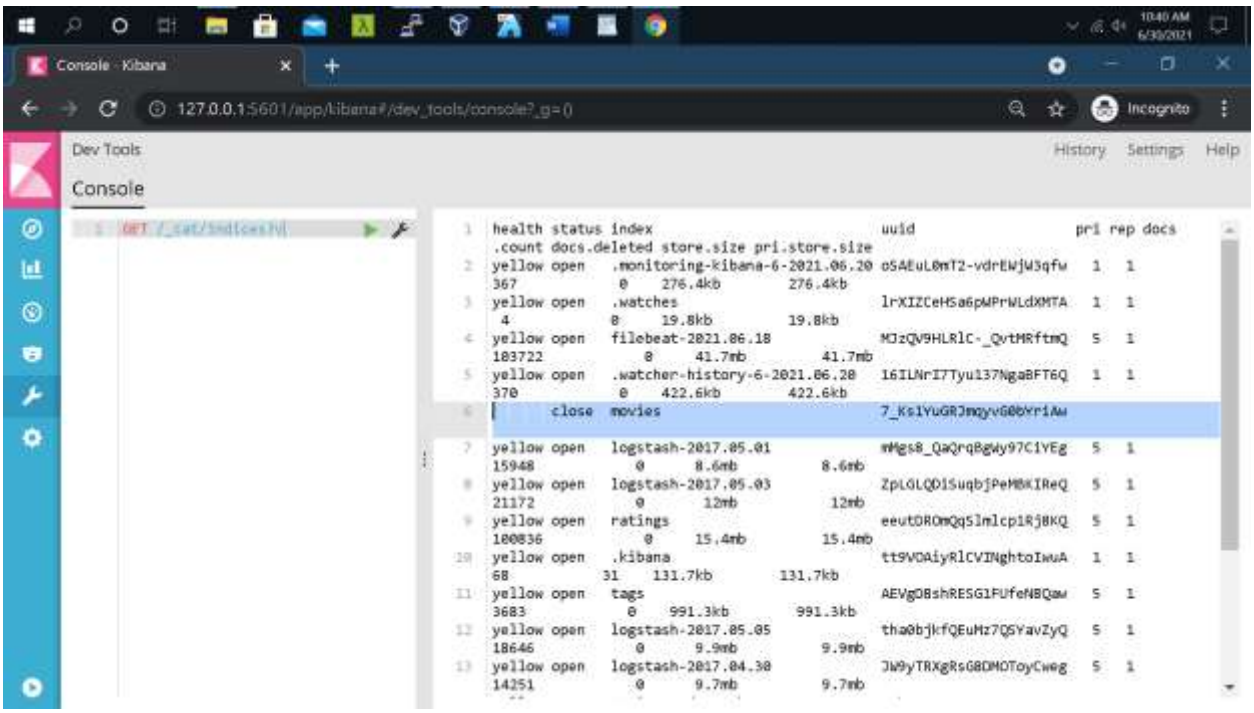


Step 9: Now to test closing and opening of index, type following command

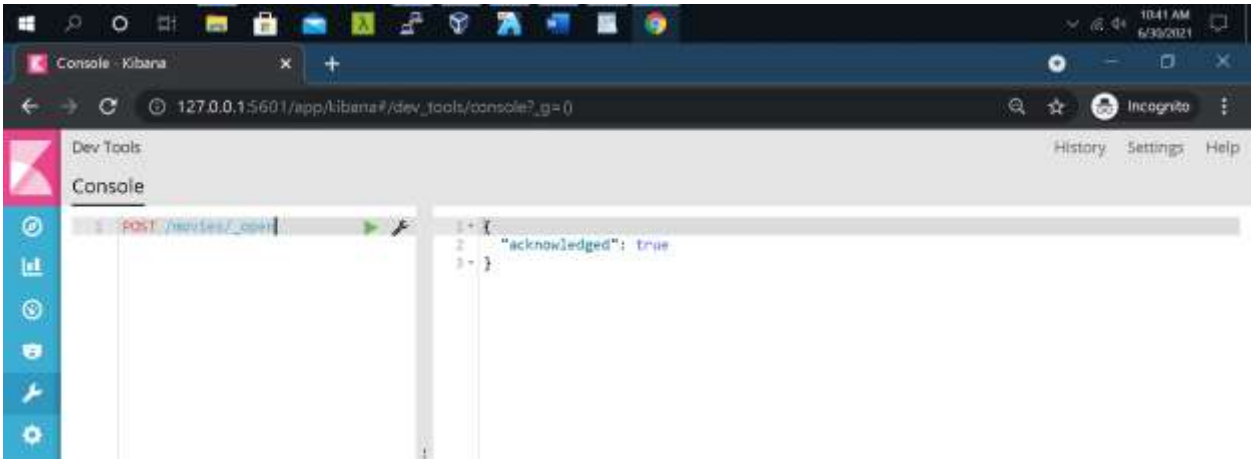
>>>POST /movies/_close



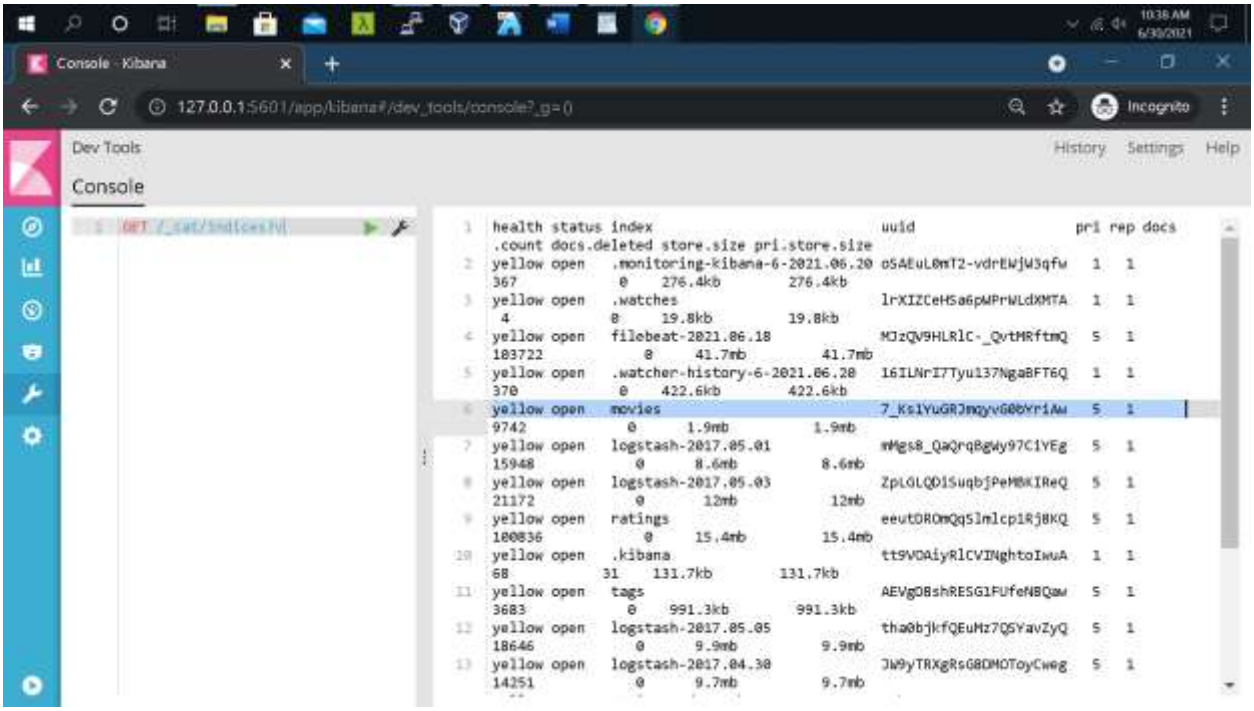
>>>GET /_cat/indices?v



>>>POST /movies/_open



>>>GET /_cat/indices?v

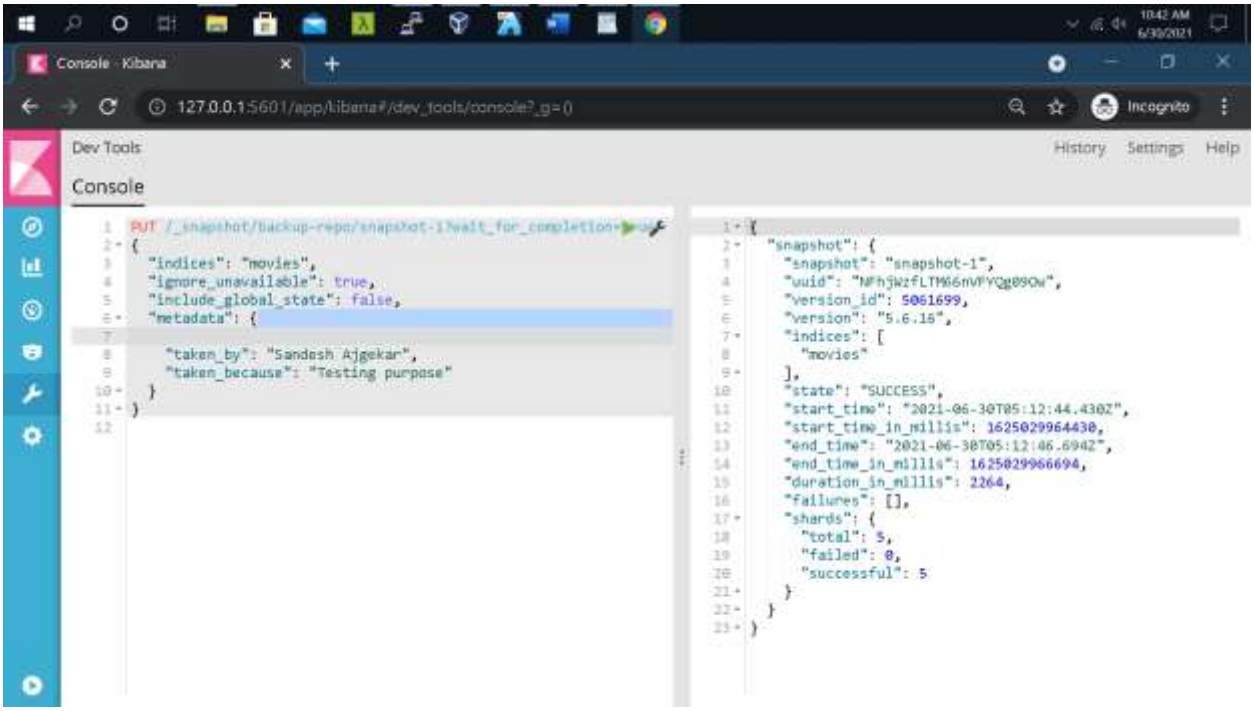


Refer: https://www.elastic.co/guide/en/elasticsearch/reference/current/indices-close.html#indices-close

https://www.elastic.co/guide/en/elasticsearch/reference/current/indices-open-close.html

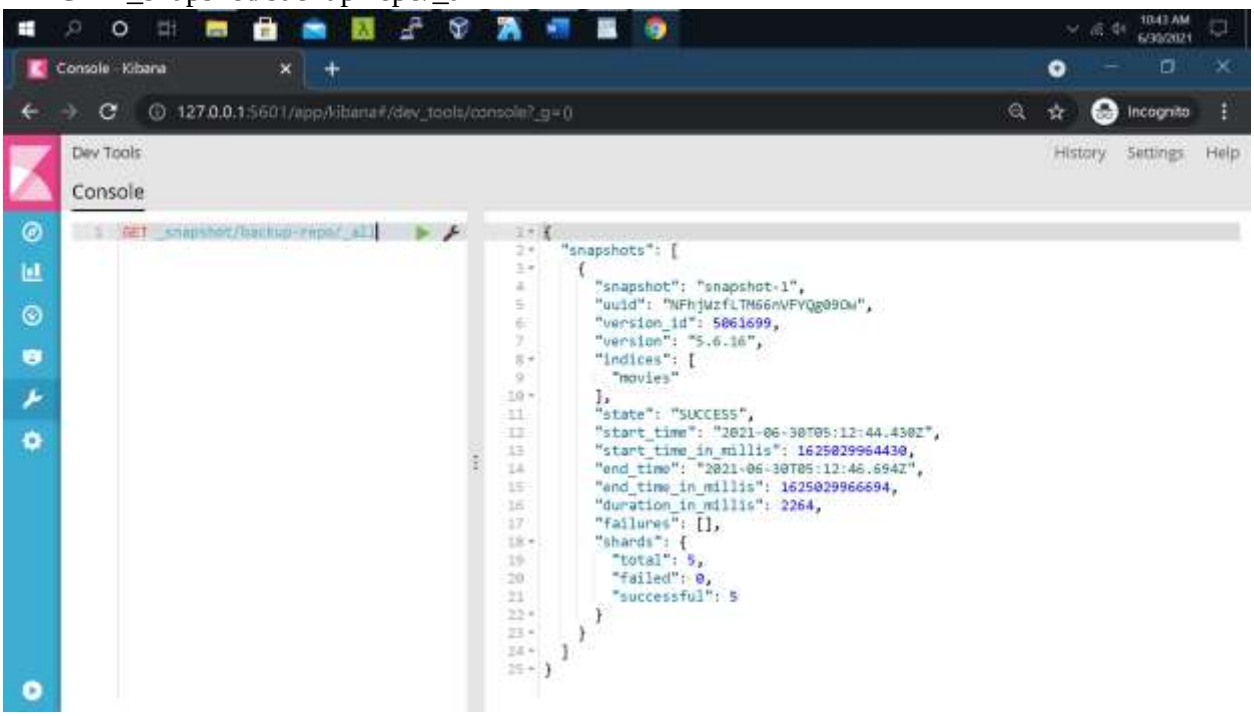
Step 10: Now take snapshot of the open index

```
>>>PUT /_snapshot/backup-repo/snapshot-1?wait_for_completion=true
{
  "indices": "movies",
  "ignore_unavailable": true,
  "include_global_state": false,
  "metadata": {
    "taken_by": "Sandesh Ajgekar",
    "taken_because": "Testing purpose"
  }
}
```



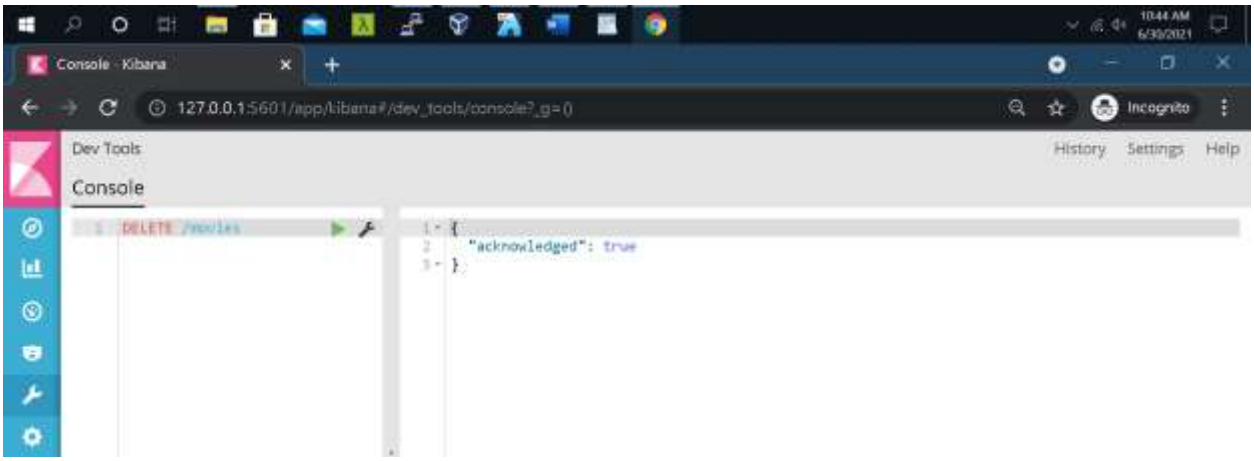
Step 11: To check snapshot, type following command

>>>GET _snapshot/backup-repo/_all

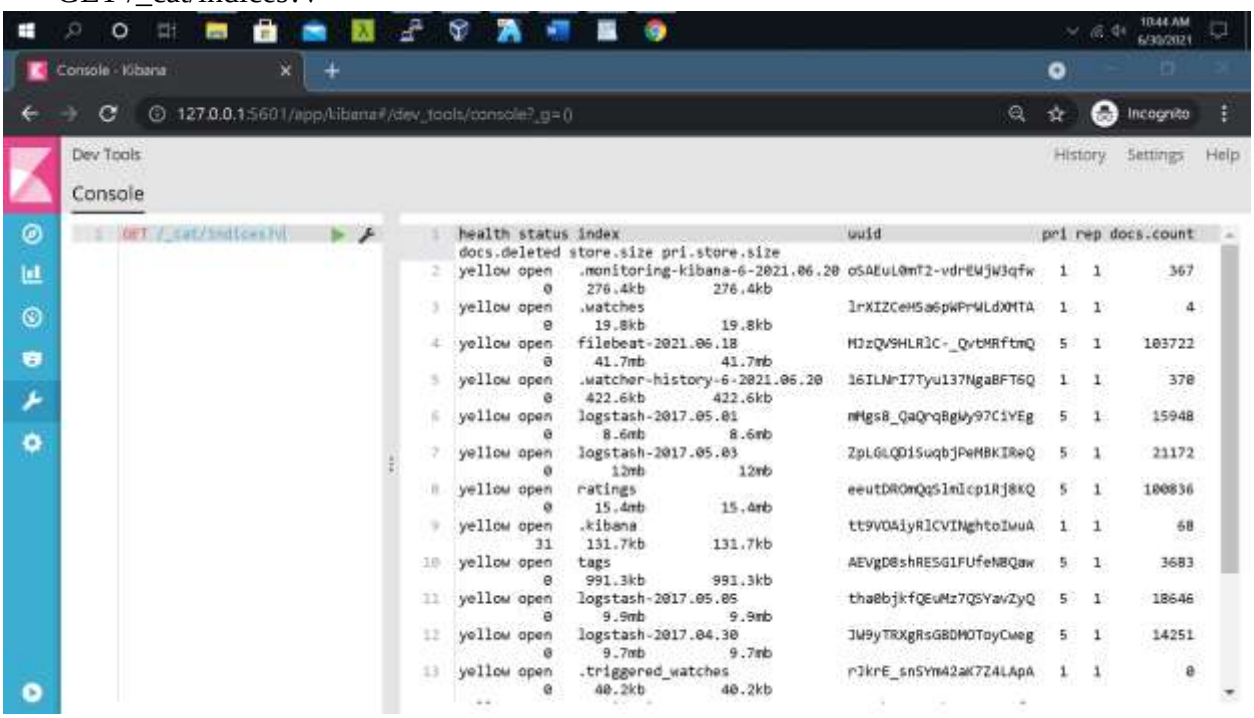


Step 12: now delete the index which snapshot have taken

>>>DELETE /movies

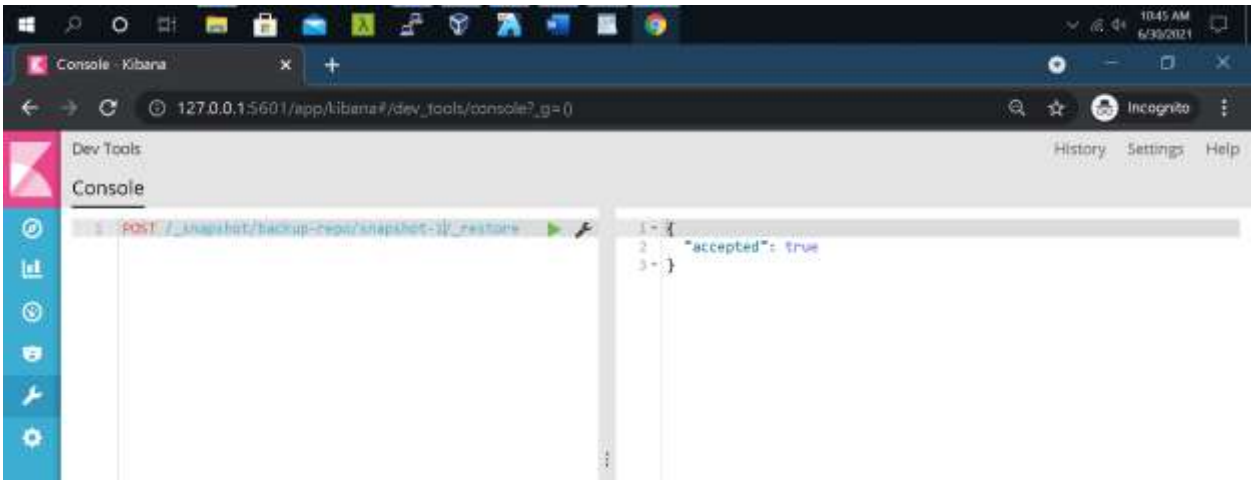


>>>GET /_cat/indices?v

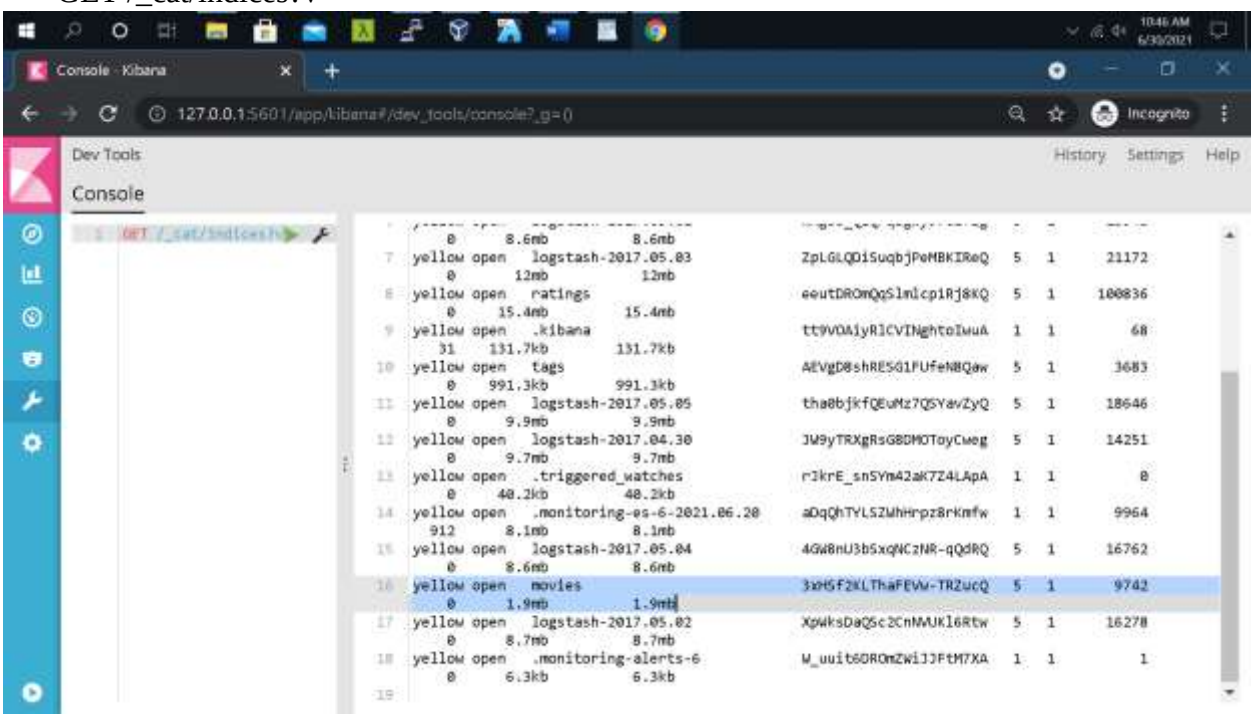


Step 13: now recover deleted index by restoring snapshot, type

>>>POST /_snapshot/backup-repo/snapshot-1/_restore



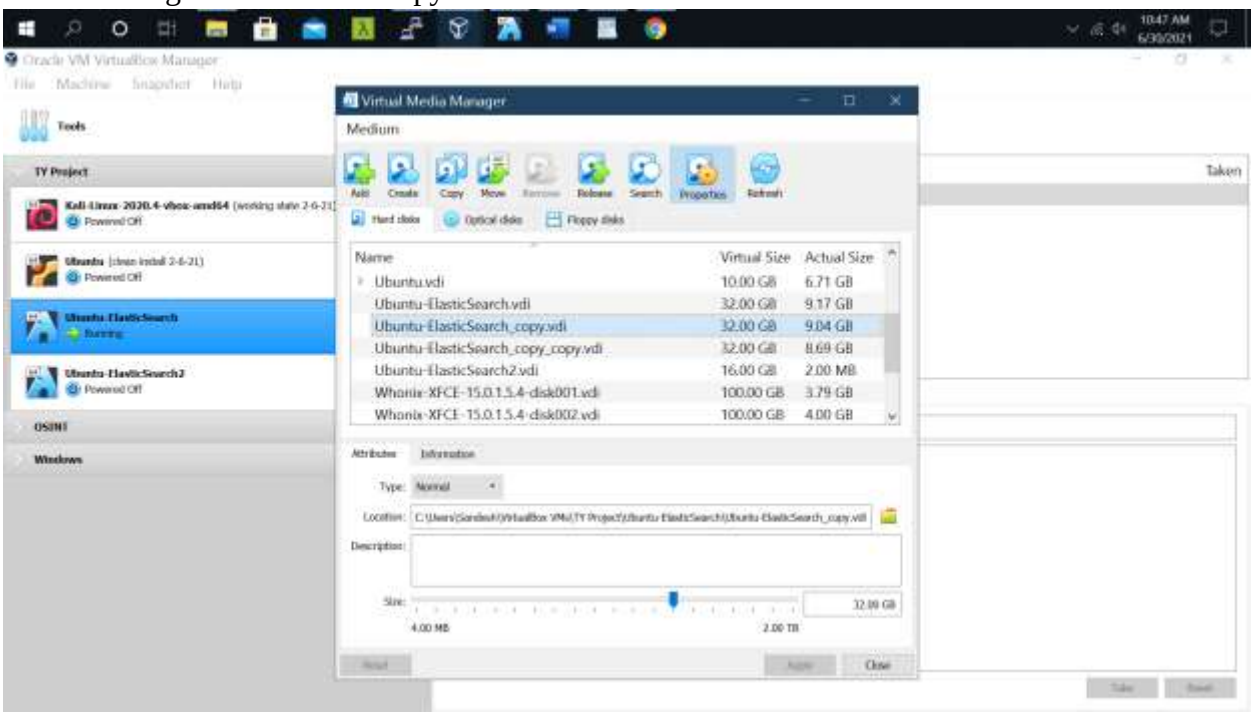
>>>GET /_cat/indices?v



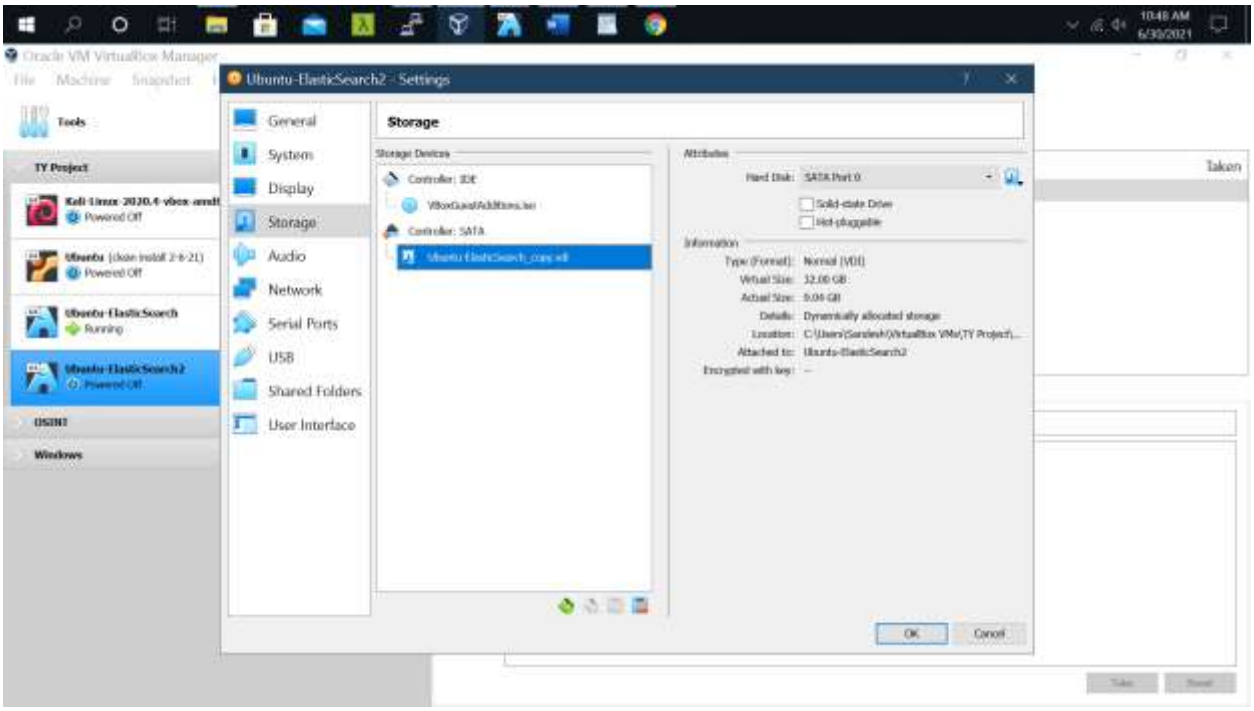
Q. How to Restore from a Snapshot from one cluster node to another cluster node?

Refer: https://qbox.io/blog/elasticsearch-data-snapshots-restore-tutorial/

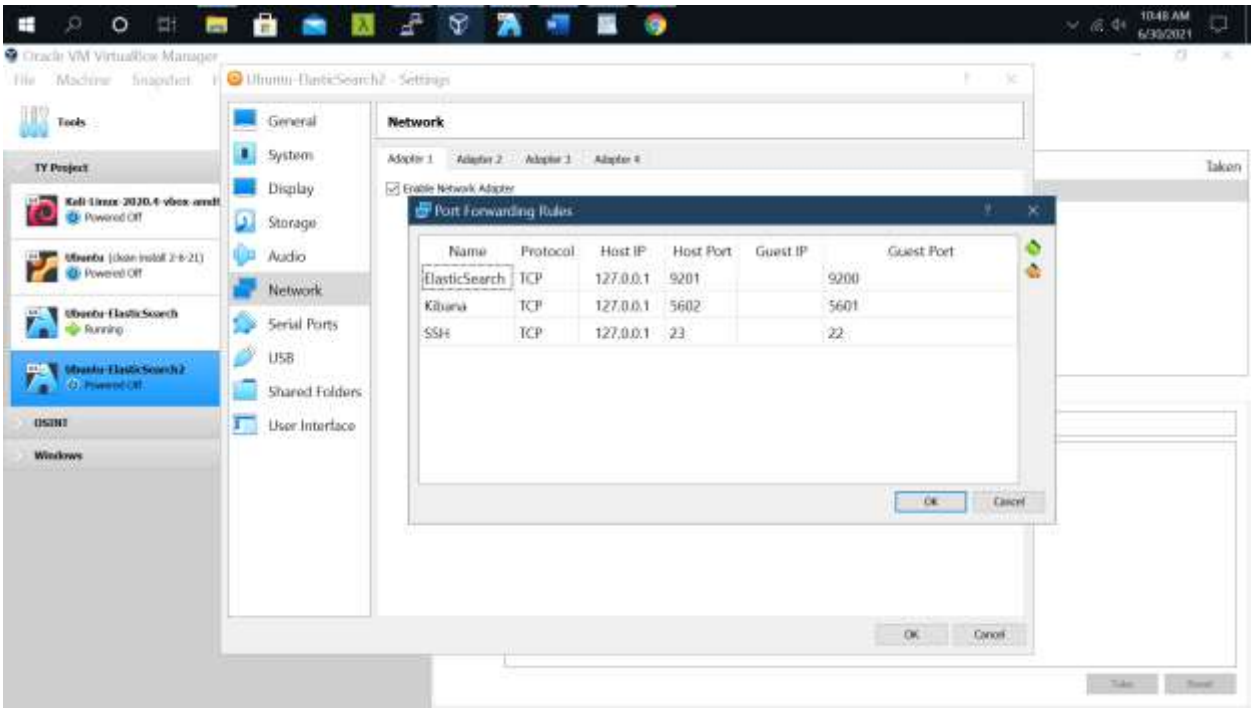
Step 0: Create entire new Elasticsearch virtual machine OR on VirtualBox go to File->Virtual Media Manager-> And make copy of vdi file of 1st Elasticsearch virtual machine.



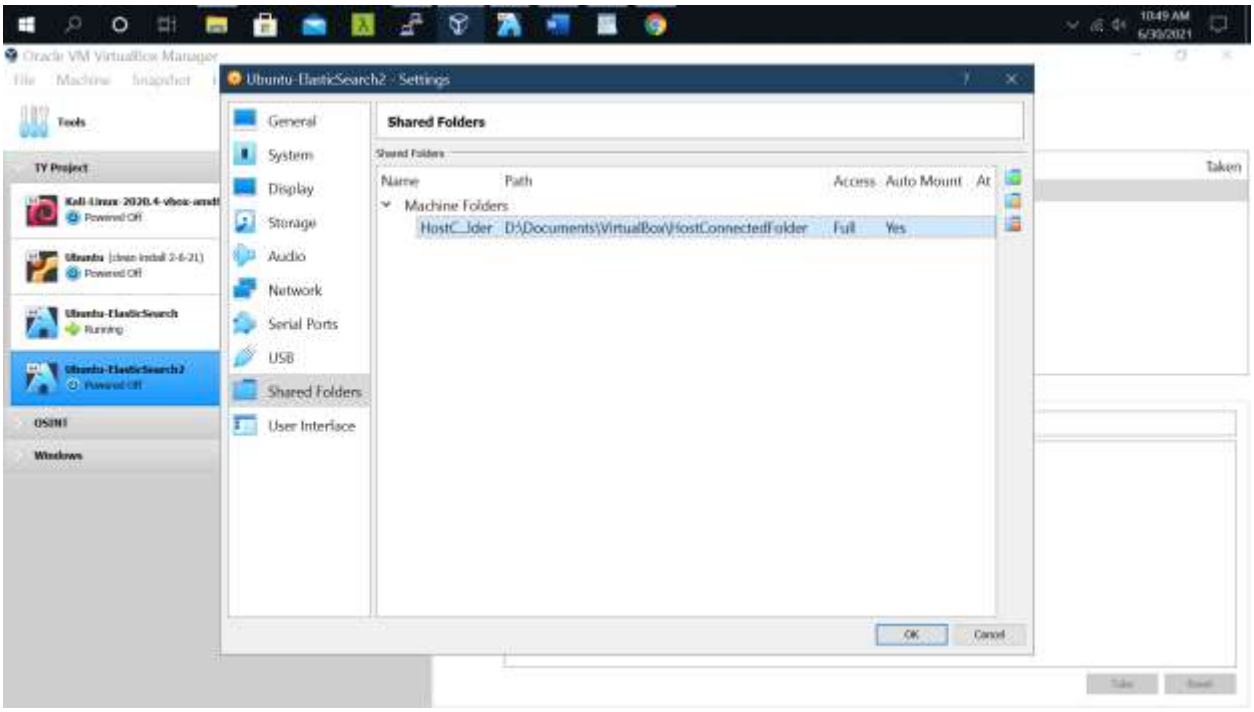
Now create another Virtual machine of name Elasticsearch 2 and go to Settings->Storage->Click on 'Controller:SATA' ->Click on 'Add Hard Disk' -> Select copy of vdi file of 1st Elasticsearch virtual machine ->Remove any other vdi file attached



Go to Network-> Advanced -> port forwarding and make sure you map different ES, Kibana, SSH ports to the local machine then 1st Elasticsearch virtual machine.



Now go to shared folders and connect any host folder to the virtual machine -> ok -> Start the Elasticsearch 2 virtual machine.



Attached same shared folder to 1st Elasticsearch virtual machine same way.

Step 1: Compress backup folder on cluster1 node OR move entire folder.

tar -zcvf backup.tar.gz ~/backups/

Step 2: Connect two VM's by shared host folder and move zip /entire folder from cluster1 to shared folder to cluster2.

```
knight@elksearch:~$ sudo cp -rp backups /media/sf_HostConnectedFolder/backups
knight@elksearch:~$
```

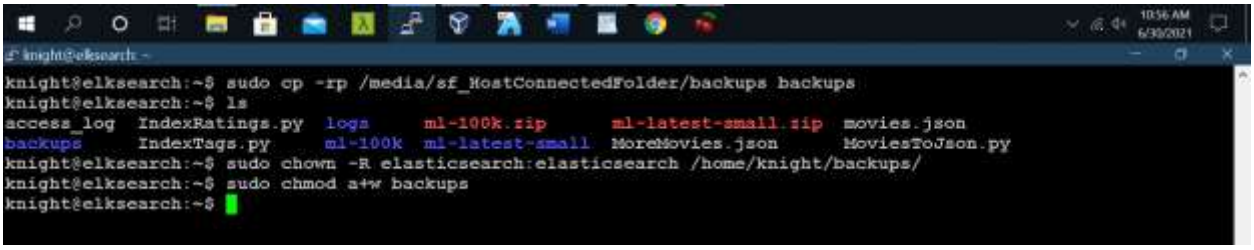
```
knight@elksearch:~$ sudo cp -rp /media/sf_HostConnectedFolder/backups backups
knight@elksearch:~$
```

Step 3: Place unzip folder/ entire folder at exact position on cluster2 as placed at cluster 1.

Step 4: Next, make sure that the Elasticsearch user has needed permissions to access the directory on cluster2 node -

$ sudo chown -R elasticsearch:elasticsearch /home/knight/backups/

$sudo chmod a+w backups

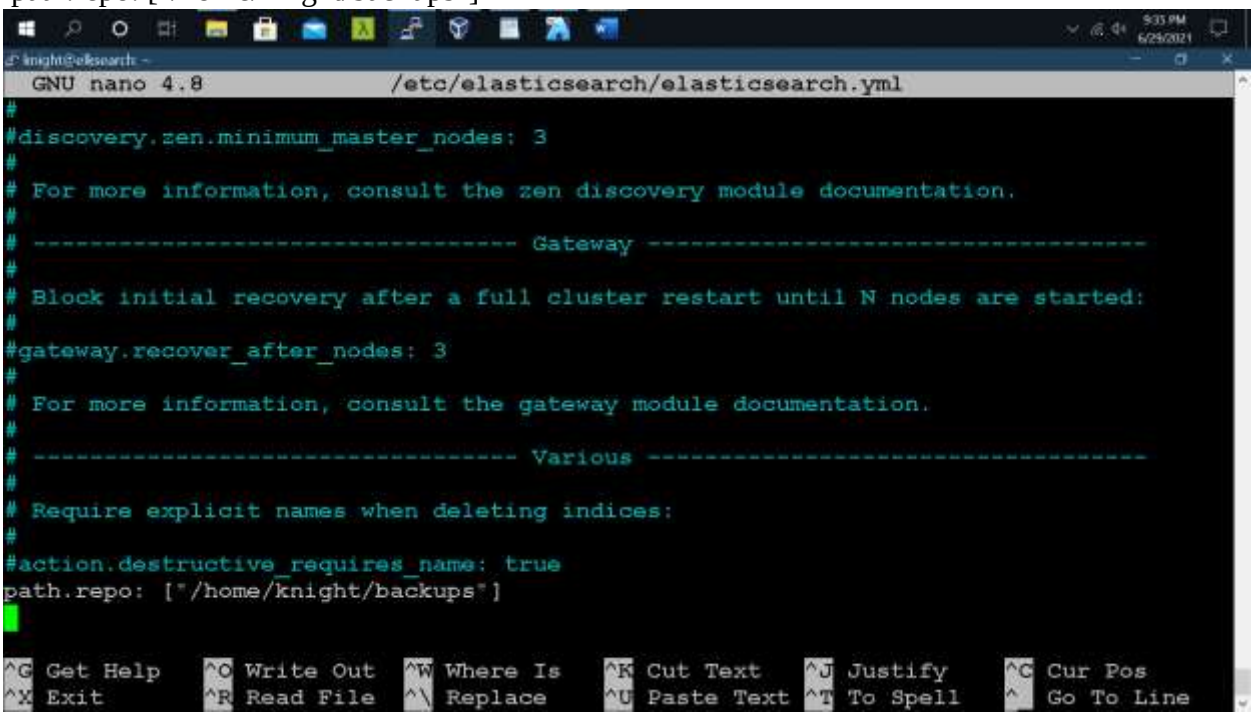


Step 5: Make entry in the .yml file of elasticsearch on cluster2 node i.e., /etc/elasticsearch/elasticsearch.yml -

$ sudo nano /etc/elasticsearch/elasticsearch.yml

Add following line at the end of the yml file,

path.repo: ["/home/knight/backups"]

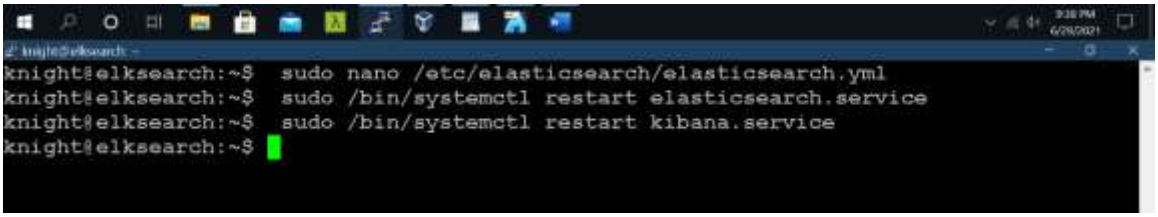


Step 6: Restart the elasticsearch service on cluster2 node -

$ sudo /bin/systemctl restart elasticsearch.service

Step 7: restart kibana on cluster2 node -

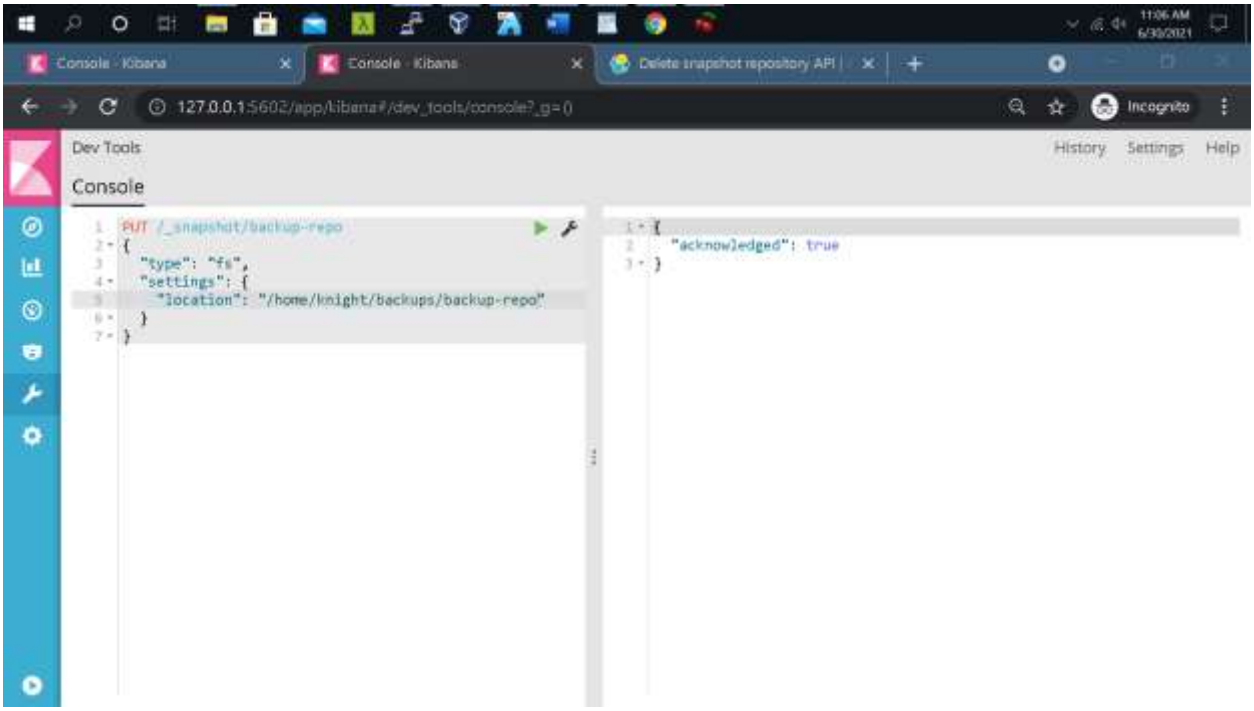
$ sudo /bin/systemctl restart kibana.service



Step 8: Now go to browser and open kibana – 127.0.0.1:5602 and open DevTool and type -

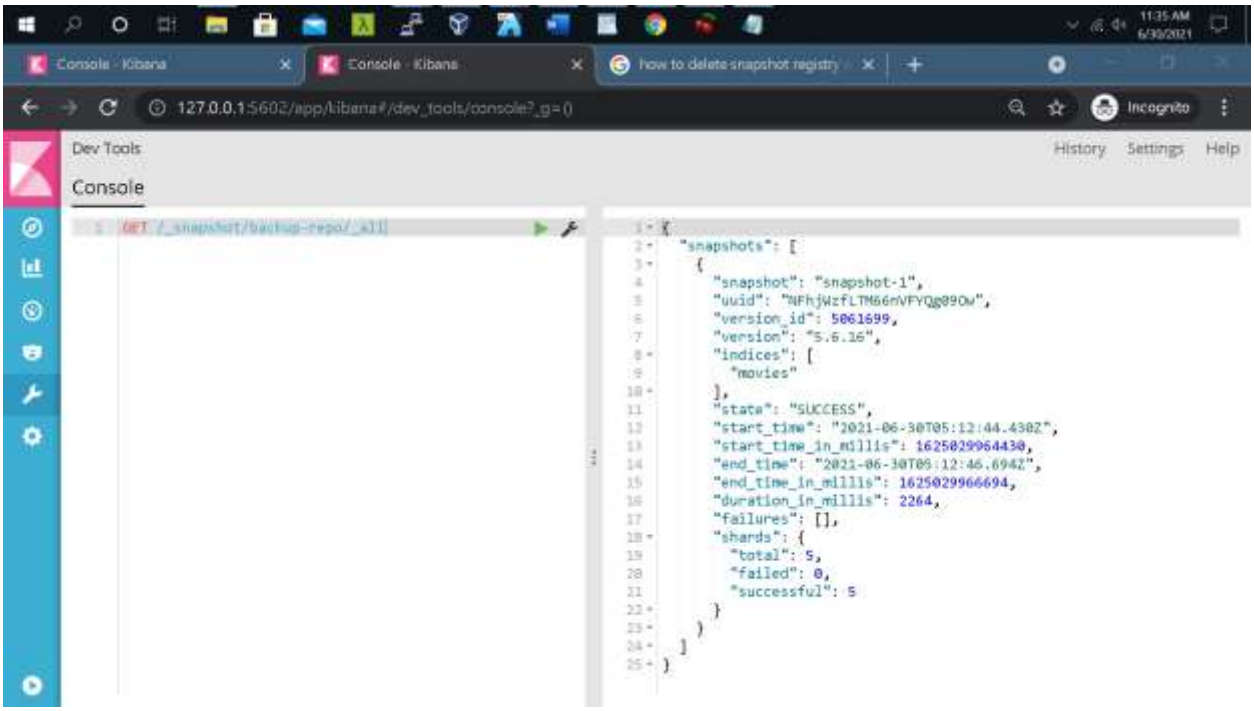
>>> PUT /_snapshot/backup-repo

```
{
  "type": "fs",
  "settings": {
    "location": "/home/knight/backup/backup-repo"
  }
```



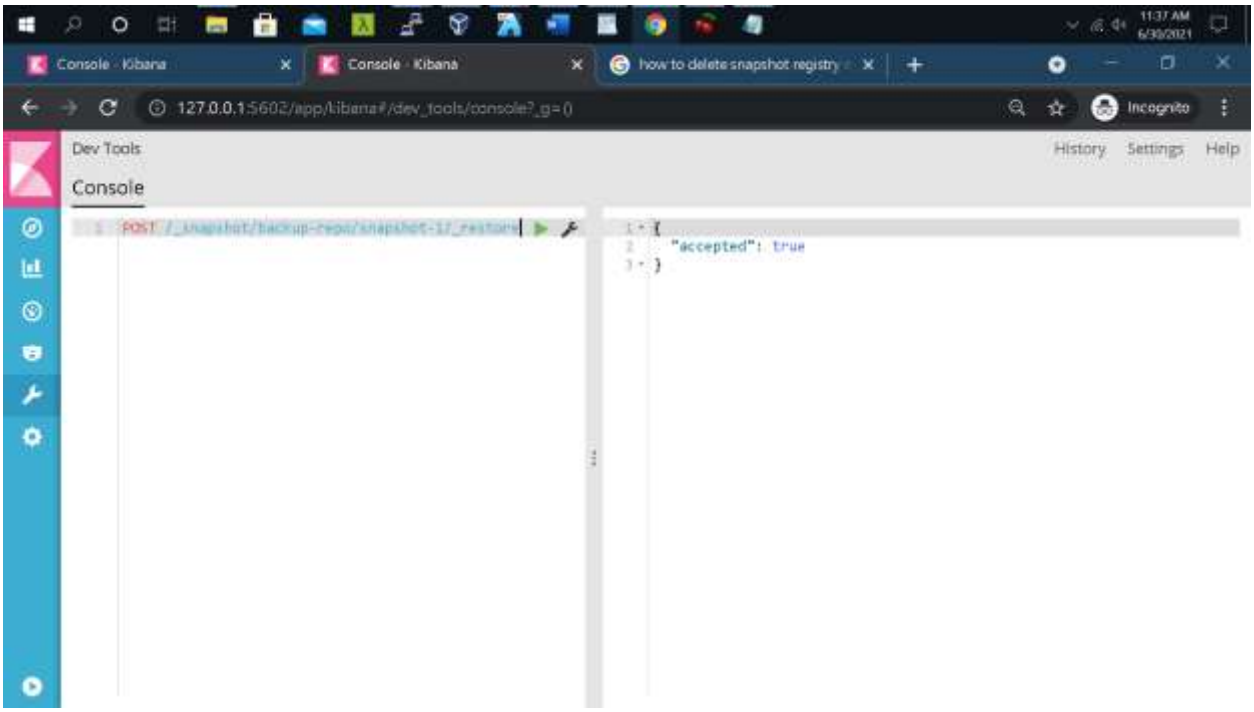
Step 9: Now list the snapshots in the repository, type -

>>>GET _snapshot/backup-repo/_all

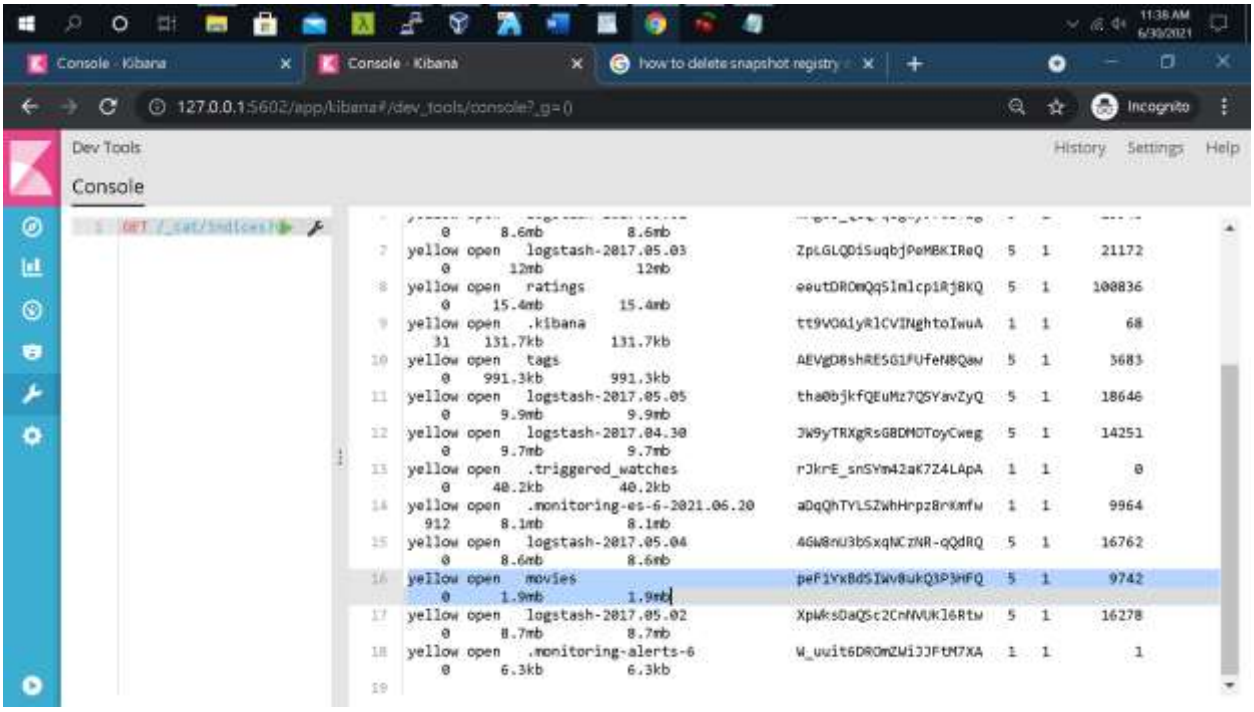


Step 10: now recover deleted index by restoring snapshot, type -

>>>POST /_snapshot/backup-repo/snapshot-1/_restore



>>>GET /_cat/indices?v



Step 11: Query any command on recovered index to view data

>>>GET /movies/_search?pretty