**Snapshot and Restore**

**Restoration of Indices in Elastic Search**

In the browser get logged in to the Elastic site by mapping the public ip : port number ie <public Ip>:5601

We will get directed to the Elastic home page. Navigate to Stack Management, then to snapshot and Restore .

Click on the snapshot tab to find the snapshots that are taken already.

Similarly repositories tab will display the repositories available.

Go to Snapshot tab ,then select the corresponding snapshot from which the restoration of indices to be done.

Then click on the restore option.

We will get navigated to a new tab, Restore snapshot.

In the data stream and indices part, enter the name of the index that you want to restore. Click next and restore.

To view the restored index in kibana, go to Dev tools and enter the following kibana command

**To view the index details**

GET /\_cat/indices

This will shows the details of all the indices in this repository including the status of the restored index

In this Red and yellow denotes a failed restoration and green denotes a successful restoration.

**To view the explanation for the restored index**

GET /\_cluster/allocation/explain

For indices with red status :

The red health status of the restored indices, it can be because of multiple reasons like crashed node, disk space issue, no replicas available to promote etc.

If we check the cluster allocation details we will get the reason for the red status like:

1.The previous copy of the primary shard existed but can no longer be found on the nodes in the cluster

For this we will have to allocate the indices manually.

**To allocate the shards to index manually**

POST filebeat-6.8.12-2021.02.24/\_settings?pretty=true

{

"commands": [

{

"move": {

"index": "filebeat-6.8.12-2021.02.24", "shard": 1,

"from\_node": "node-1", "to\_node": "node-2"

}

}

]

}

This can be done only if we have more than one nodes in our cluster.But in our case only one node is available in the cluster “ cloud\_elastic”. Then while checking the allocation details will get the following

2.Cannot allocate because allocation is not permitted to any of the nodes.

Elasticsearch never assigns the replica of the same primary shard on the same node for high availability reasons. And we have only one node in our cluster.

****S**olutions**

1.Add more nodes to your cluster, so that replicas can be assigned on other nodes. (preferred way)

2.Reduce the replica shards to 0, this can cause data-loss and performance issues. (if at all, you don't have the option to add data-nodes and you want the green state for your cluster).

**Changing the number of replicas.**

PUT filebeat-6.8.12-2021.02.24/\_settings

{

"index" : {

"number\_of\_replicas" : 0

}

}

This will result in a successful restoration of index in Elastic search.