**Reindexing data on Elastic Search**

1. Create new index with mapping

**PUT http://10.97.252.12:9200/copyto\_v1**

**{**

**"mappings": {**

**"copyto" : {**

**"properties": {**

**"attack": {**

**"type": "string",**

**"index": "not\_analyzed"**

**},**

**"attack1": {**

**"type": "string",**

**"index": "not\_analyzed",**

**"copy\_to": [**

**"attack"**

**]**

**},**

**"attack2": {**

**"type": "string",**

**"index": "not\_analyzed",**

**"copy\_to": [**

**"attack"**

**]**

**},**

**"attack3": {**

**"type": "string",**

**"index": "not\_analyzed"**

**},**

**"eventid": {**

**"type": "string"**

**}**

**}**

**}**

**}**

**}**

**}**

1. Copy data from old index to new using

<https://github.com/garbin/elasticsearch-reindex>

<https://www.npmjs.com/package/npm>

On the Elasticsearch node, download npm and node.js and run these commands

**npm install -g elasticsearch-reindex**

**elasticsearch-reindex -f http://10.97.252.12:9200/copyto/copyto -t http://10.97.252.12:9200/copyto\_v1/copyto**

1. Create/Update alias to point to new index

**POST http://10.97.252.12:9200/\_aliases**

**{**

**"actions" : [**

**{ "add" : { "index" : "copyto\_v1", "alias" : "copy" } }]**

**}**

1. Delete old index

**DELETE** [**http://10.97.252.12:9200/copyto**](http://10.97.252.12:9200/copyto)

1. Check data on Kibana

**PUT http://10.97.252.12:9200/\_snapshot/my\_backup**

**{**

**"type": "fs",**

**"settings": {**

**"location": "C:\\ESBackup\\my\_backup",**

**"compress": true**

**}**

**}**

1. Add this line on ES node in the file elasticsearch.yml under the “Paths” section

**path.repo : ["C:\\\\ESBackup"]**

1. Create a snapshot to rename the newly created index

**PUT http://10.97.252.12:9200/\_snapshot/my\_backup/snapshot\_20160426**

**{**

**"indices": "copyto\_v1",**

**"ignore\_unavailable": "true",**

**"include\_global\_state": false**

**}**

1. Verify the snapshot

**GET http://10.97.252.12:9200/\_snapshot/my\_backup/snapshot\_20160426**

1. Close the index which needs to be restored

**POST http://10.97.252.12:9200/copyto\_v1/\_close**

1. Restore from snapshot

**POST http://10.97.252.12:9200/\_snapshot/my\_backup/snapshot\_20160426/\_restore**

**{**

**"indices": "copyto\_v1",**

**"ignore\_unavailable": "true",**

**"include\_global\_state": false,**

**"rename\_pattern": "(copyto)\_v1",**

**"rename\_replacement": "$1"**

**}**

1. Open the index

**POST** [**http://10.97.252.12:9200/copyto\_v1/\_open**](http://10.97.252.12:9200/copyto_v1/_open)

1. Verify there are 2 indexes – copyto and copyto\_v1 and check the shards value.

**GET** [**http://10.97.252.12:9200/\_cat/indices**](http://10.97.252.12:9200/_cat/indices)

1. Delete the old index and start using the restored one.

**DELETE** [**http://10.97.252.12:9200/copyto\_v1**](http://10.97.252.12:9200/copyto_v1)