Elasticsearch Cheat Sheet

update_by_query

```
POST /index/_update_by_query
{
  "script": "ctx._source.field = 'correct value'",
  "query": {
    "term": {
      "field": "wrong value"
    }
  }
}
```

backup

Add backup directory to repository

```
$ grep backup /srv/elk/elasticsearch/config/elasticsearch.yml
path.repo: [ "/backup" ]
```

Register snapshot repository

```
PUT /_snapshot/backup
{
  "type": "fs",
  "settings": {
    "location": "/backup",
    "compress": "true"
  }
}
```

Create snapshot

```
PUT /_snapshot/backup/snapshot_$date?wait_for_completion=true
```

Prune Indices with curator

```
$ cat action.yml
actions:
  1:
```

```
    action: delete_indices
    description: >-
      Delete indices older than 5 days (based on index name), for logstash-
      prefixed indices. Ignore the error if the filter does not result in an
      actionable list of indices (ignore_empty_list) and If you want to
change the retention Days then goto unit_count:<enter no of day>.
    options:
      ignore_empty_list: True
      timeout_override:
      continue_if_exception: False
      disable_action: False
    filters:
    - filtertype: pattern
      kind: prefix
      value: logstash-
      exclude:
    - filtertype: age
      source: name
      direction: older
      timestring: '%Y.%m.%d'
      unit: days
      unit_count: 90
      exclude:

$ cat config.yml
client:
  hosts:
    - elk-elasticsearch
  port: 9200
  url_prefix:
  use_ssl: False
  certificate:
  client_cert:
  client_key:
  ssl_no_validate: False
  http_auth:
  timeout: 30
  master_only: False

logging:
  loglevel: INFO
  logfile:
  logformat: default
  blacklist: ['elasticsearch', 'urllib3']

$ curator --config ./config.yml action.yml
```

Merge smaller indexes to one large index

```
$ curl --netrc --insecure --request POST --header "Content-Type:
```

```
application/json" https://elk-elasticsearch:9200/_reindex -d'
{
  "source": {
    "index": "filebeat-7.13.2-2021.07.*"
  },
  "dest": {
    "index": "filebeat-7.13.2-2021.07-000001"
  }
}'

$ curl --netrc --insecure --request PUT --header "Content-Type:
application/json"
https://elk-elasticsearch:9200/filebeat-7.13.2-2021.07-000001/_alias/filebea
t-7.13.2
```

kb, elasticsearch