

Elasticsearch 7.x Cheatsheet

All the API endpoints and pro-tips you always forgot about in one place!
Built by developers for developers. Hosted on [GitHub](#), contributions welcome.



Links

First thing, forget about your `curl` calls and **install Kibana** please !

- [Download Elasticsearch](#), official download page;
- [Elasticsearch Reference](#), official documentation;
- [Awesome Elasticsearch](#), curated list of resources about ES;
- [Official forum](#) and [StackOverflow](#) for support;
- to help upgrading the stack.

Queries

There are two syntaxes for the basic queries: a simple one on the left, where you can't use any option, and an extended one on the right. Most of the beginner headache with the DSL come from this:

GET _search

```
{
  "query": {
    "match": {
      "FIELD": "TEXT"
    }
  }
}
```

TO

GET _search

```
{
  "query": {
    "match": {
      "FIELD": {
        "query": "TEXT",
        "OPTION": "VALUE"
      }
    }
  }
}
```

Full search example with aggregation, highlight, filter...

GET /_search

```
{
  "query": {
    "bool": {
      "must": [
```

```
{
  "match": {
    "title": "smith"
  }
},
"must_not": [
  {
    "match_phrase": {
      "title": "granny smith"
    }
  }
],
"filter": [
  {
    "exists": {
      "field": "title"
    }
  }
]
},
"aggs": {
  "my_agg": {
    "terms": {
      "field": "user",
      "size": 10
    }
  }
},
"highlight": {
  "pre_tags": [
    "<em>"
  ],
  "post_tags": [
    "</em>"
  ],
  "fields": {
    "body": {
      "number_of_fragments": 1,
      "fragment_size": 20
    },
    "title": {}
  }
}
```

```
    },
    "size": 20,
    "from": 100,
    "_source": [
        "title",
        "id"
    ],
    "sort": [
        {
            "_id": {
                "order": "desc"
            }
        }
    ]
}
```

Control total hit count

Accept true, false or a fixed number, default to 10000.

GET /_search

```
{
  "track_total_hits": true,
  "query": {}
}
```

Common queries

```
"multi_match": {
  "query": "Elastic",
  "fields": ["user.*", "title^3"],
  "type": "best_fields"
}
```

```
"bool": {
  "must": [],
  "must_not": [],
  "filter": [],
  "should": [],
  "minimum_should_match" : 1
}
```

```
"range": {
  "age": {
    "gte": 10,
    "lte": 20,
```

```
"boost": 2
}
```

QueryString syntax recap

Search in the default `_all` field:

```
GET /_search?q=pony
```

Complex search with operator and exact phrase search with boost:

```
GET /_search?q=title:(joli OR code) AND author:"Damien Alexandre"^2
```

Search with wildcard and special queries:

```
GET /_search?q=_exists_:title OR title:singl? noneOrAnyChar*cter
```

Search with fuzzyness and range:

```
GET /_search?q=title:elastichurch~3 AND date:[2016-01-01 TO 2018-12-31]
```

Use in Query DSL (not recommended for user search):

```
GET /_search
{
  "query": {
    "query_string": {
      "default_field": "content",
      "query": "elastic AND (title:lucene OR title:solr)"
    }
  }
}
```

Indexes and mapping

Create an index with settings and mapping

```
PUT /my_index_name
{
  "settings": {
    "number_of_replicas": 1,
    "number_of_shards": 3,
    "analysis": {},
  }
}
```

```
"refresh_interval": "1s"
},
"mappings": {
  "properties": {
    "title": {
      "type": "text",
      "analyzer": "english"
    }
  }
}
```

Types are deprecated, you can only use one in Elasticsearch 6.

Update index settings dynamically

PUT /my_index_name/_settings

```
{
  "index": {
    "refresh_interval": "-1",
    "number_of_replicas": 0
  }
}
```

Update an index by adding a field to a type

PUT /my_index_name/_mapping

```
{
  "properties": {
    "tag": {
      "type": "keyword"
    }
  }
}
```

Get the mapping and the settings

GET /my_index_name/_mapping

GET /my_index_name/_settings

Create a document (auto-generated ID)

POST /my_index_name/_doc

```
{  
  "title": "Elastic is funny",  
  "tag": [  
    "lucene"  
  ]  
}
```

Create or update a document**PUT /my_index_name/_doc/12abc**

```
{  
  "title": "Elastic is funny",  
  "tag": [  
    "lucene"  
  ]  
}
```

Delete a document

DELETE /my_index_name/_doc/12abc

Open and close indexes to save memory and CPU

POST /my_index_name/_close

POST /my_index_name/_open

Remove and create aliases**POST /_aliases**

```
{  
  "actions": [  
    {  
      "remove": {  
        "index": "my_index_name",  
        "alias": "foo"  
      }  
    },  
    {  
      "add": {  
        "index": "my_index_name",  
        "alias": "bar",  
      }  
    }  
  ]  
}
```

```
    "filter" : { "term" : { "user" : "damien" } }  
  }  
}  
]  
}
```

List aliases

GET /_aliases

GET /my_index_name/_alias/*

GET /*/_alias/*

GET /*/_alias/foo

Full custom analyzer declaration

PUT /english_example

```
{  
  "settings": {  
    "analysis": {  
      "filter": {  
        "english_stop": {  
          "type": "stop",  
          "stopwords": "_english_"  
        },  
        "english_stemmer": {  
          "type": "stemmer",  
          "language": "english"  
        }  
      },  
      "analyzer": {  
        "my_english": {  
          "char_filter": ["html_strip"],  
          "tokenizer": "standard",  
          "filter": [  
            "lowercase",  
            "english_stop",  
            "english_stemmer"  
          ]  
        }  
      }  
    }  
  }  
}
```

```
}  
}
```

Indices monitoring and information

GET /my_index_name/_stats

GET /my_index_name/_stats

GET /my_index_name/_segments

GET /my_index_name/_recovery?pretty&human

Indices status and management

POST /my_index_name/_cache/clear

POST /my_index_name/_refresh

POST /my_index_name/_flush

POST /my_index_name/_forcemerge

Reindex API

Simple Reindex Operation

POST /_reindex

```
{  
  "source": {  
    "index": "test-index"  
  },  
  "dest": {  
    "index": "test-index-new"  
  }  
}
```

POST /_reindex

```
{  
  "source": {  
    "index": "test-index"  
  },  
  "dest": {  
    "index": "test-index-new"  
  }  
}
```



```
}  
}
```

Selective Reindex Operation

POST /_reindex

```
{  
  "source": {  
    "index": "test-index",  
    "query": {  
      "match": {  
        "gender": "female"  
      }  
    }  
  },  
  "dest": {  
    "index": "test-index-new",  
    "type": "female"  
  }  
}
```

Debug and development

Queries

Get a detailed view of what a query do:

GET /blog/_validate/query?explain=true

```
{  
  "query": {  
    "match": {  
      "title": "Smith"  
    }  
  }  
}
```

Get an explanation about a document matching or not:

GET /blog/_doc/1/_explain

```
{  
  "query": {  
    "match": {  
      "title": "Smith"  
    }  
  }
```

```
}  
}
```

Analysis

Test how a content is tokenized in a field:

```
GET /blog/_analyze  
{  
  "field": "title",  
  "text": "powerful"  
}
```

Test analyzer token output by analyzer:

```
GET /blog/_analyze  
{  
  "analyzer": "english",  
  "text": "powerful"  
}
```

Cluster management and plugins

Cluster and node information

```
GET /_cluster/health?pretty
```

```
GET /_cluster/health?wait_for_status=yellow&timeout=50s
```

```
GET /_cluster/state
```

```
GET /_cluster/stats?human&pretty
```

```
GET /_cluster/pending_tasks
```

```
GET /_nodes
```

```
GET /_nodes/stats
```

```
GET /_nodes/nodeId1,nodeId2/stats
```

Moving shards manually

Ask the index my_index_name shard 0 of node1 to go to node2:

POST /_cluster/reroute

```
{
  "commands": [
    {
      "move": {
        "index": "my_index_name",
        "shard": 0,
        "from_node": "node1",
        "to_node": "node2"
      }
    },
    {
      "allocate": {
        "index": "my_index_name",
        "shard": 1,
        "node": "node3"
      }
    }
  ]
}
```

Updating settings

Change dynamically the minimum number of nodes to allow a master election, both persistent or not:

PUT /_cluster/settings

```
{
  "persistent": {
    "discovery.zen.minimum_master_nodes": 3
  }
}
```

PUT /_cluster/settings

```
{
  "transient": {
    "discovery.zen.minimum_master_nodes": 2
  }
}
```

Disable shard allocation, useful before a rolling restart:

PUT /_cluster/settings

```
{
  "transient" : {
```

```
    "cluster.routing.allocation.enable" : "none"
  }
}

PUT /_cluster/settings
{
  "transient" : {
    "cluster.routing.allocation.enable" : "all"
  }
}
```

Most useful plugins

Site plugins are no longer supported, look at Kibana applications or other standalone app like [Cerebro](#) for basic management.

Analysis ICU

Adding useful tokenizer and token filters from the Unicode ICU library.

```
bin/elasticsearch-plugin install analysis-icu
```

AWS Cloud

Allow discovery and storage in Amazon cloud (EC2 and S3).

```
bin/elasticsearch-plugin install discovery-ec2
```

```
bin/elasticsearch-plugin install repository-s3
```

Azure Cloud

Allow discovery and storage in Microsoft Azure cloud.

```
bin/elasticsearch-plugin install discovery-azure-classic
```

```
bin/elasticsearch-plugin install repository-azure
```

Plugins management

```
bin/elasticsearch-plugin install file:///path/to/plugin
```

```
bin/elasticsearch-plugin list
```

```
bin/elasticsearch-plugin remove [pluginname]
```

Other information

Where to find the plugin binary?

RPM: /usr/share/elasticsearch/bin

Debian: /usr/share/elasticsearch/bin

What are the default ports?

Kibana: <http://localhost:5601/>.

Elasticsearch: <http://localhost:9200/>.

How to set the correct HEAP SIZE value?

The best value for a single purpose Elasticsearch server is **about 50% of available RAM but under 32g**.

Assuming Ubuntu / Debian server, you can change those files:

/etc/security/limits.conf

```
elasticsearch - nofile 65535
elasticsearch - memlock unlimited
```

/etc/default/elasticsearch (on CentOS/RH: /etc/sysconfig/elasticsearch)

```
ES_HEAP_SIZE=20g
MAX_OPEN_FILES=65535
MAX_LOCKED_MEMORY=unlimited
```

Useful settings to change in elasticsearch.yml

```
cluster.name: jolicluster
node.name: ${HOSTNAME} # by default

network.host: [_local_, _site_]
plugin.mandatory: analysis-icu
node.data: true
node.master: true
node.ingest: true
bootstrap.memory_lock: true
action.auto_create_index: +aaa*, -bbb*, +ccc*, -*

discovery.seed_hosts:
  - 192.168.1.10:9300
  - 192.168.1.11
  - seeds.mydomain.com

# Needed for first cluster boot
cluster.initial_master_nodes:
  - 10.0.10.101
  - 10.0.10.102:9300
  - 10.0.10.102:9301
  - master-node-name
```

```
# Disable X-Pack features
xpack.security.enabled: false
xpack.monitoring.enabled: false
xpack.ml.enabled: false
xpack.watcher.enabled: false
xpack.sql.enabled: false
xpack.graph.enabled: false
```