Elasticsearch Search and analytics engine

CONCEPTS

Reading this sheet
Entries are METHOD path. Run them as curl -X <METHOD> $ES/<path>, with --json '<body>' when a body is given (curl 7.82+ sets the JSON headers), or paste them into Kibana Dev Tools. Set ES=localhost:9200 first.

Elasticsearch 8+ enables security by default: use ES=https://localhost:9200 and add -u elastic:<password> --cacert <http_ca.crt> to every curl.

CLUSTER AND CAT

`GET /`
Node name, cluster, version

`GET _cluster/health?pretty`
Green / yellow / red status

`GET _cat/indices?v`
Indices with docs and size

`GET _cat/nodes?v`
Nodes and load

INDICES

`PUT <index>`
Create an index

`DELETE <index>`
Delete an index and its data

`GET <index>/_mapping`
Show field mappings

DOCUMENTS

`POST <index>/_doc`
Index with a generated id

`PUT <index>/_doc/<id>`
Index or replace by id

`GET <index>/_doc/<id>`
Get a document

`DELETE <index>/_doc/<id>`
Delete a document

DOCUMENTS (cont.)

`POST <index>/_update/<id>`
Partial update: {"doc":{...}}

SEARCH

`GET <index>/_search?q=<field>:<text>`
URI search for quick checks

`POST <index>/_search`
Search with a query body

`{"match": {"<field>": "<text>"}}`
Full-text match

`{"term": {"<field>": "<value>"}}`
Exact value (keyword, number)

`{"bool": {"must": [], "filter": [], "must_not": []}}`
Combine clauses

`{"range": {"<field>": {"gte": 10, "lt": 20}}}`
Range filter

`"size": 20, "from": 40`
Paginate

`"sort": [{"<field>": "desc"}]`
Sort results

AGGREGATIONS

`"size": 0, "aggs": {"by": {"terms": {"field": "<f>"}}}`
Top values (terms)

`{"avg": {"field": "<field>"}}`
Metric: avg, min, max, sum

`{"date_histogram": {"field": "<f>", "calendar_interval": "day"}}`
Count per day

BULK AND REINDEX

`POST _bulk`
Many writes, NDJSON body

`POST _reindex`
Copy: {"source":{...},"dest":{...}}