ELK

## Introduction

This document covers

Introduction

## 10,000 Feet View

What is Elastic Search?

Key Features?

* Based on Lucene and uses inverted index
* Documents are JSON.
* Indexes, Documents and Fields

#### Elasticsearch Commands

|  |  |  |
| --- | --- | --- |
|  | Example | Description |
| Add Document | PUT /kennydocs/\_doc/audi  {  "color" : "whitee",  "model" : "a3"  } | Known as indexing the document |
| Replace document | PUT /kennydocs/\_doc/audi  {  "color" : "whitee",  "model" : "a3",  "make" : "audi"  } | Documents are immutable so a copy in inserted over the existing one with the changed fields |
| Update document | POST /kennydocs/\_doc/audi  {  "year" : 2002  } | Again note documents are immutable so this copies existing fields and add the new field |
| Retrieve by id with meta data | GET /kennydocs/\_doc/audi | {  "\_index" : "kennydocs",  "\_type" : "\_doc",  "\_id" : "audi",  "\_version" : 3,  "\_seq\_no" : 2,  "\_primary\_term" : 1,  "found" : true,  "\_source" : {  "color" : "whitee",  "model" : "a3",  "make" : "audi"  }  } |
| Retrieve by id without meta data | GET /kennydocs/\_doc/audi/\_source | {  "color" : "whitee",  "model" : "a3",  "make" : "audi"  } |
| Check if document exists | HEAD /kennydocs/\_doc/audi | 200 – OK |
| Delete document | DELETE /kennydocs/\_doc/audi | Delete document |
| Get index structure | GET /kennydocs |  |
| Delete index | DELETE /kennydocs |  |
| Match All | GET /kennydocs/\_search  {  "query": {  "match\_all": {}  }  } |  |
| Search | GET /kennydocs/\_search  {  "query": {  "term": {  "color": {  "value": "whitee"  }  }  }  } |  |

## Overview

In Elastic documents are stored in indices. Each document is composed of fields.

### Commands

#### Add a document (Indexing)

We add a document as follows. The index in this case is kennydocs and the id of the document is audi. Every document must have an id. If we do not provide one elastic will create one for us.

PUT /kennydocs/\_doc/audi

{

"color" : "whitee",

"model" : "a3"

}

#### Updating a document

If we update the document, we use the same id.

PUT /kennydocs/\_doc/audi

{

"color" : "whitee",

"model" : "a3",

"make" : "audi"

}

And we get the response as follows. Note the version is increased.

{

"\_index" : "kennydocs",

"\_type" : "\_doc",

"\_id" : "audi",

"\_version" : 2,

"result" : "updated",

"\_shards" : {

"total" : 2,

"successful" : 1,

"failed" : 0

},

"\_seq\_no" : 2,

"\_primary\_term" : 1

}

## LogStash

## Appendices

Install Windows

#### Install Java

The first step is to make sure we have Java 1. 8 installed. You can get this from the Sun site

<https://www.java.com/en/download/>

#### Get Specific version of Elasticsearch

<https://www.elastic.co/downloads/past-releases/elasticsearch-6-3-2>

and unzip into a folder

#### Run Elasticsearch

Install instructions <https://www.elastic.co/downloads/elasticsearch>

For this version we need to change line 46 of bin/elasticsearch.bat - from %JAVA% to !JAVA!

Now we run it using.

bin/elasticsearch.bat

And check it running using

curl <http://localhost:9200/>

{

"name" : "14vDG6A",

"cluster\_name" : "elasticsearch",

"cluster\_uuid" : "4AAe6vjJTx-naXoZz5Gl7g",

"version" : {

"number" : "6.3.2",

"build\_flavor" : "default",

"build\_type" : "zip",

"build\_hash" : "053779d",

"build\_date" : "2018-07-20T05:20:23.451332Z",

"build\_snapshot" : false,

"lucene\_version" : "7.3.1",

"minimum\_wire\_compatibility\_version" : "5.6.0",

"minimum\_index\_compatibility\_version" : "5.0.0"

},

"tagline" : "You Know, for Search"

}

#### Get Specific version of Kibana

Get specific version of Kibana.

<https://www.elastic.co/downloads/past-releases/kibana-6-3-2>

Install instructions.

<https://www.elastic.co/downloads/kibana>

Uncomment line 28 of kibana.yml

elasticsearch.url: "http://localhost:9200"

Run bin/kibana.bat

Open URL

<http://localhost:5601/app/kibana>