## ELK\_20-2-2025

A diagram of a diagram

AI-generated content may be incorrect.

we can add the data through different ways in elasticsearch via logstash, filebeat, fluentbit, shellscript, python script or devtools and etc

we are using the dev tools to insert and interact with the data here

A screenshot of a computer

AI-generated content may be incorrect.

Use this grokdebugger for <https://grokdebugger.com> or the one within the dev tools

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

# Creating Index and adding document to the index

We created the sample index

A screenshot of a computer

AI-generated content may be incorrect.

After putting the index the shard got increased from 69

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.under the sandwich menu > stack management > indexmanagement you can see my-index

A screenshot of a computer

AI-generated content may be incorrect.

There are multiple options when you select a index

Click on delete index for now

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

You can use devtools to delete the index as well

A screenshot of a computer

AI-generated content may be incorrect.

For now we will put the index again and add the document to the my-index

It created 2 shards as well

Whenever you get a success, you will get a 201 response which means created response

A screenshot of a computer

AI-generated content may be incorrect.

# Data view

If you want to see above data

Click on sandwich menu > click stack management > under Data click on the Index Management

Copy this index name from there and you will have to create a data view



Scroll down on on Stack management on the left > under Kibana click on the Data Views

Click on create dataview, if there are none.

A screenshot of a computer

AI-generated content may be incorrect.

You will get the view below for after click Create Data View, in there name your dataview, the index pattern that needs to be matched on for the alias rollover when the ILM runs for data retention

A screenshot of a computer

AI-generated content may be incorrect.

Index pattern by matching which sources you want it to be matched on.

Currently we don’t have the Timestamp field in our index document, we will be adding data time to the document within the index for it be matching the index so the timestamp field is allowed. For now we are just going to save the data view as is without the date to our document

A screenshot of a computer

AI-generated content may be incorrect.

Whatever is starting with the \_ is the metadata field, meta data is field which is generated by the system not by our data which we have sent to the document.

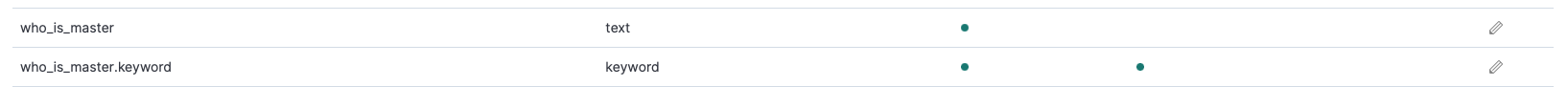
\_source is not searchable

Text field is not aggregable but my keyword is aggregatble

A screenshot of a computer

AI-generated content may be incorrect.

It is keeping both data type with text and keyword (this is the concept of tokenization, where in one form all the strings are sliced and searchable in other case the strings aren’t completely sliced before saving {do homework on this})



Relationship shows

A screenshot of a computer

AI-generated content may be incorrect.

To Visualize this data, you have to click on sandwich menu > Under Analytics click on Discover

A screenshot of a computer

AI-generated content may be incorrect.

Since we haven’t provided the data time field, we see there is no time stamp

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

If you delete the index, the dataview will still be there because we have created the dataview with the index pattern and it is not able to see anything.

A screenshot of a computer

AI-generated content may be incorrect.

# @timestamp field

A screenshot of a computer

AI-generated content may be incorrect.

We can add this to add the date time to our index when posting the document inside it

|  |
| --- |
| POST my-index-name/\_doc  {  "message": "User signed up",  "@timestamp": "2025-05-01T10:15:30Z"  } |

Elastic search uses the GMT time format, it converts the local time to the GMT format.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

The date time is still not appearing as the timestamp for us to look back on, so for that we will have to edit the dataview and select Timestamp field.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a chat

AI-generated content may be incorrect.

As you can see the @timestamp available

A screenshot of a computer

AI-generated content may be incorrect.

As you can see you can now select the timestamp calendar to see the date with the document.

A screenshot of a computer

AI-generated content may be incorrect.

Let’s suppose that if my master is down what will happen? You have 3 elasticsearch servers on which elastic is running. In our case minimum 2 elasticsearch nodes are required so in this case the master will switch (they will have internal election called quorum)

### 🔸 What is a Quorum Election?

When a new master is needed (e.g., cluster startup or master failure), Elasticsearch holds an **election** among the **master-eligible nodes**. To prevent split-brain scenarios (i.e., two nodes thinking they're master), it uses a **quorum-based voting system**.

#### ✅ Quorum = (N / 2) + 1

Where **N** = total number of **master-eligible nodes**

For example:

* If you have 3 master-eligible nodes → Quorum = **2**
* If you have 5 nodes → Quorum = **3**

A node can only become master if it **gets votes from a quorum** of the other master-eligible nodes.

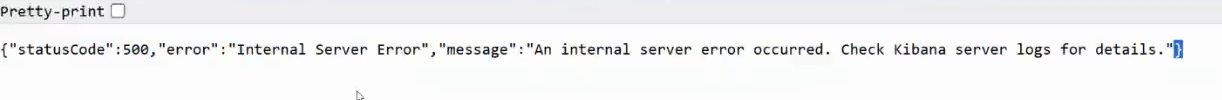
So our current master is node-2

A screenshot of a computer

AI-generated content may be incorrect.

As you can see behind the terminal the node-1 has become the master and node-2 is offline A screenshot of a computer

AI-generated content may be incorrect.

if I bring any other elasticsearch node down, we will have an error and it will not operate, because for multi-cluster architect you need minimum 2 elasticsearch nodes. We will bring all our servers up. But if all your servers are down, you will have to bring the master node up first whomever was a last master. 

bring all the server sequentially starting with the last master and your cluster should be up and running.

Or

You can master eligible nodes, then the cluster will work