# Discovering Kibana

## Devtools

A screenshot of a computer

AI-generated content may be incorrect.

## Stack management

A screenshot of a computer

AI-generated content may be incorrect.

## Stack monitoring

You can setup a monitoring with Metricbeat if you have installed and configured it, or else, you can turn click on “ Or, set up with self monitoring “

A screenshot of a computer

AI-generated content may be incorrect.

click on turn on monitoring

A screenshot of a computer error

AI-generated content may be incorrect.

## Cluster overview

A screenshot of a computer

AI-generated content may be incorrect.

This dashboard gives you cluster overview

If you notice the Health says it is missing replica shards, it is because we have created we didn’t create the replica node when we pushed the index from the dev tool previously.

go through what each tile and understand what is happening.

“Document count is 629” because we turned on the monitoring previously and that is why some data is getting written to the elasticsearch related to monitoring matrix and the document count is increasing

Related to the document it has automatic cleanup capability

Disk usage is 3.9

Primary shards is 35

Replica shards is 0

Q: Why replica shard is 0?

A: if we are running with the single node, all the shards are going reside on the single node server. It will not make sense to create the replica shard, it wont make sense for elasticsearch.

A screenshot of a computer

AI-generated content may be incorrect.

If I were to place 2 nodes, then the replica will be created. That is why primary shards are 35 and replica shards are 0.

A screenshot of a computer

AI-generated content may be incorrect.

# go through all the tiles and understand what they mean.

Click on indices tile

A screenshot of a computer

AI-generated content may be incorrect.

Again this is index is showing up because, this is the index we posted from devtools in previous step. Look at all the information.

We will also understand the Unassigned shard as well.

A screenshot of a computer

AI-generated content may be incorrect.

9300 is the transport port and it is running on 127.0.0.1 server (local)

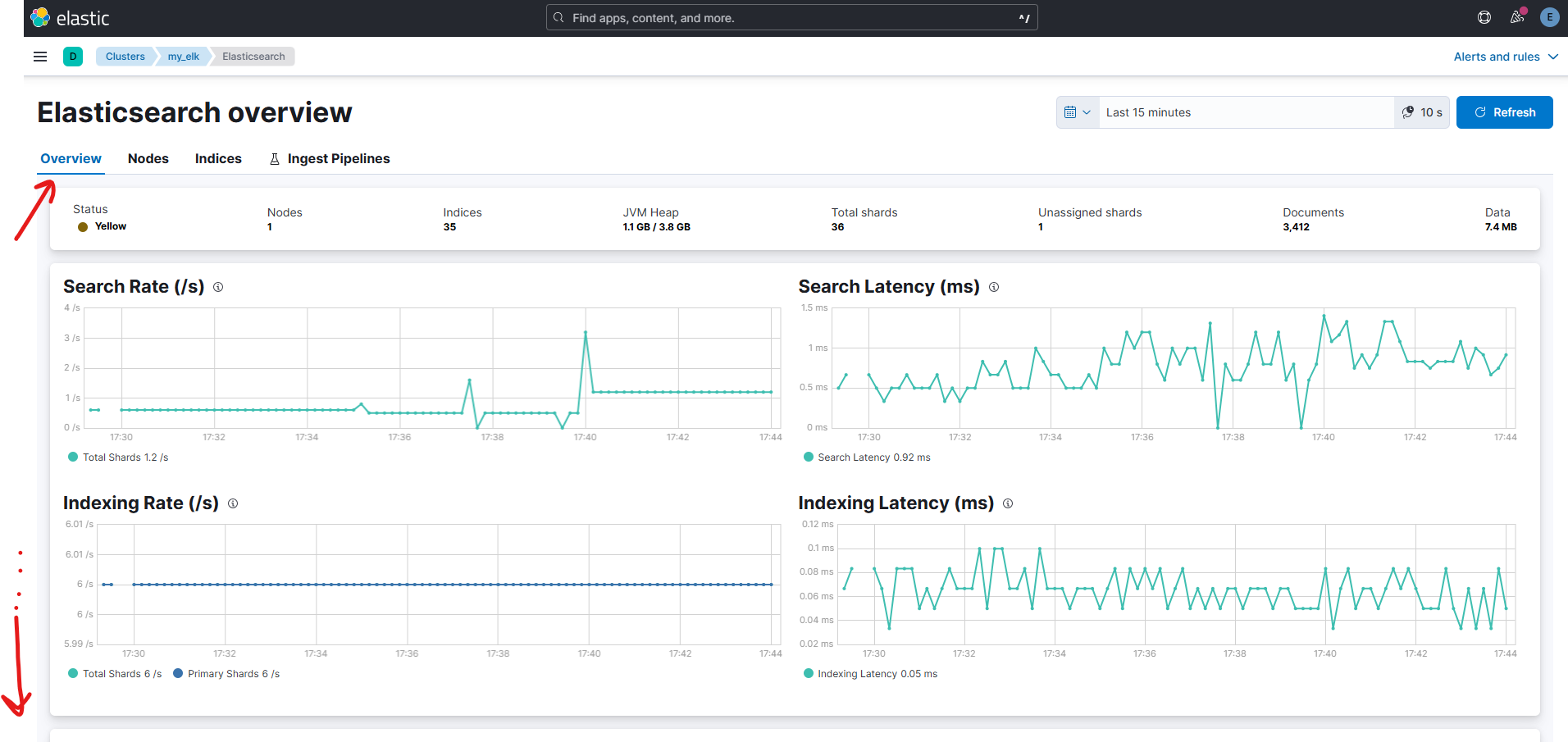
The reason transport port is being used is because of the data exchange from the elasticsearch; on which data gets transported from one node to another node.

Discover all the options like alerts, status, roles, shards, cpu usage, load average… etc

A screenshot of a computer

AI-generated content may be incorrect.

Click on overview and it will show you the cluster monitoring metrics, scroll down



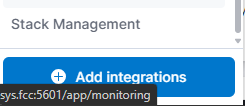
Turn on shard activity completed recoveries and you will see more activities.

A white rectangular object with text

AI-generated content may be incorrect.

Click on hamburger/sandwich menu on top left next to default space > scroll down > click on stack management

It will give you more control over the elastic search.



Within stack management “Data” is one of the important places where you manage your cluster data and backups. It helps you created index components/template and settings. Life cycle policies for retentions etc

Go through all the menu options and discover.

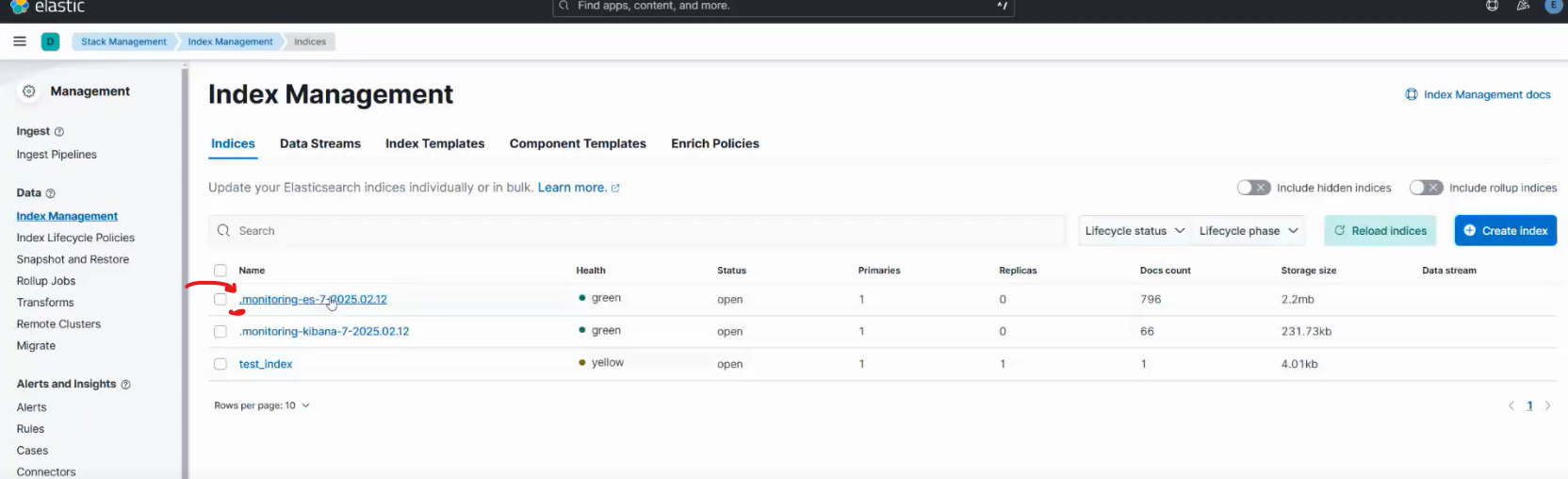
A screenshot of a computer

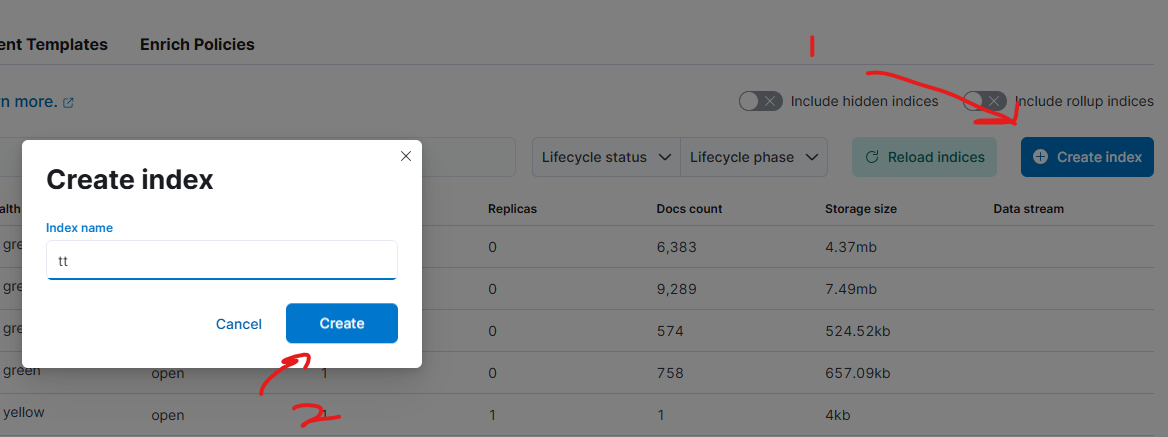
AI-generated content may be incorrect.

Whichever indices that starts with the . (dot) are the system indices. System managed, Elasticsearch itself is managing these indexes. (index is one, indices means many)

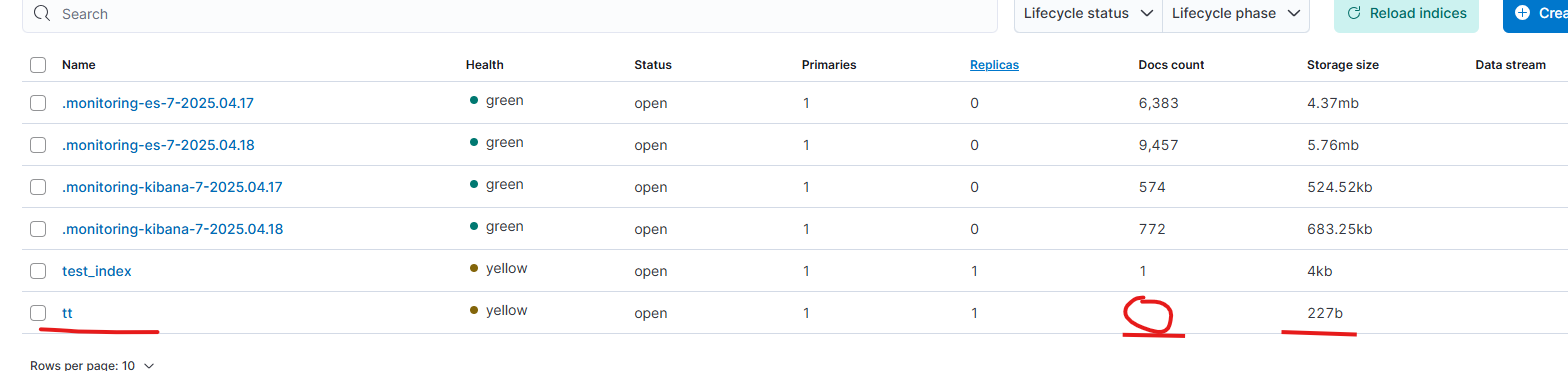
And indices that starts without the . (dot) are the regular indices that’s been logged

You can also create index by click on the create index



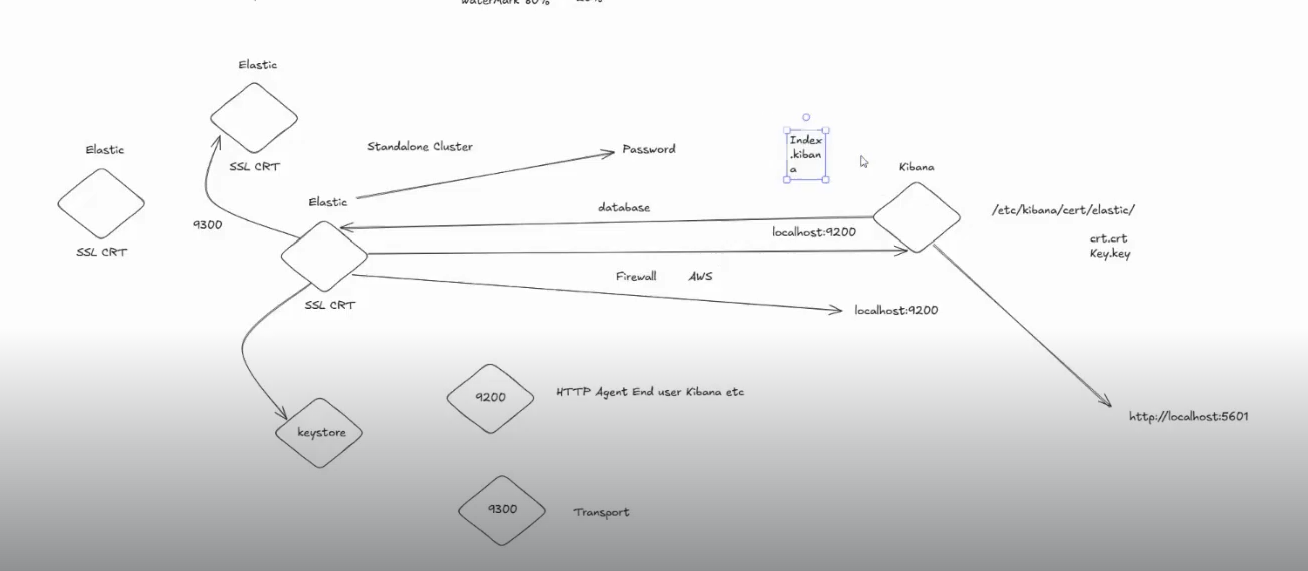


There are zero documents with empty data with some metadata.



# Index Management

Index is a information container

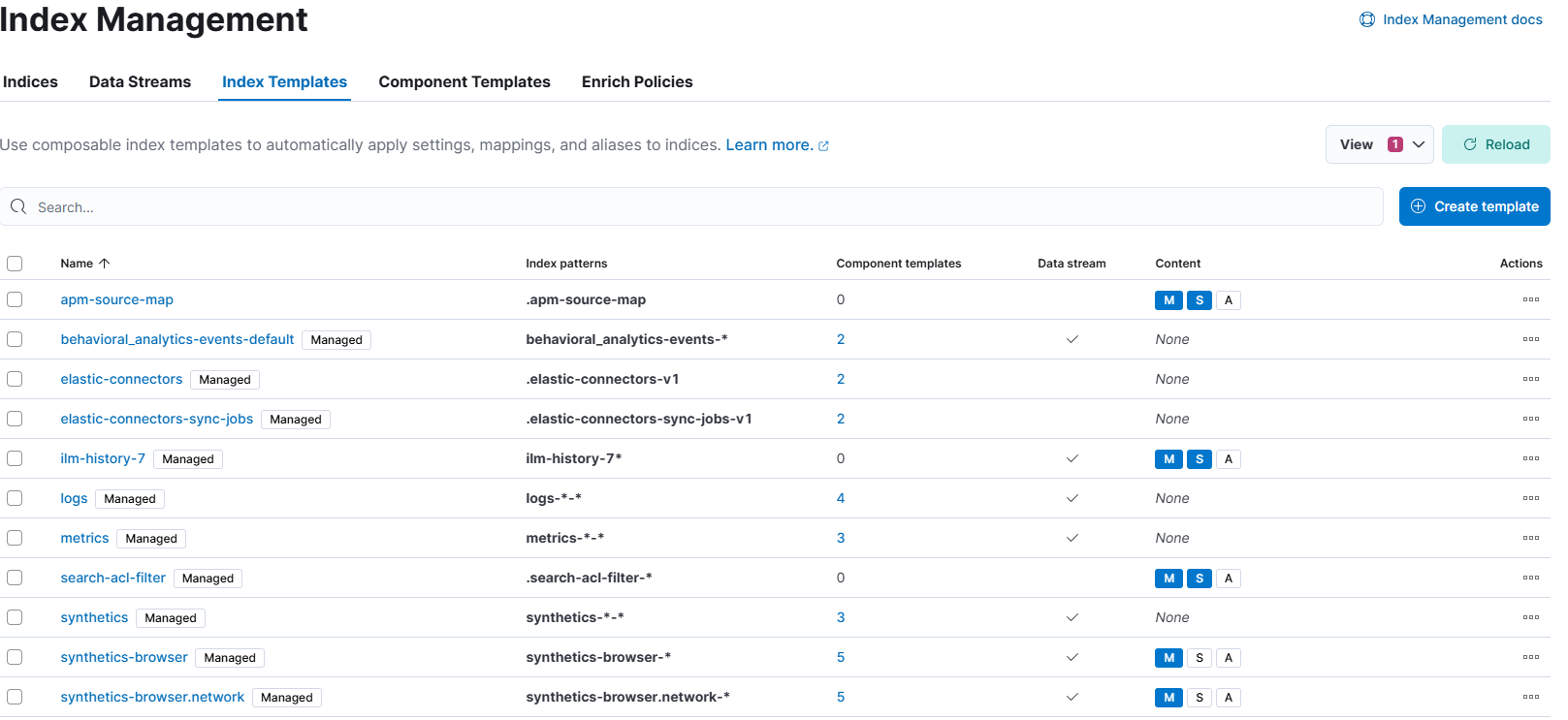


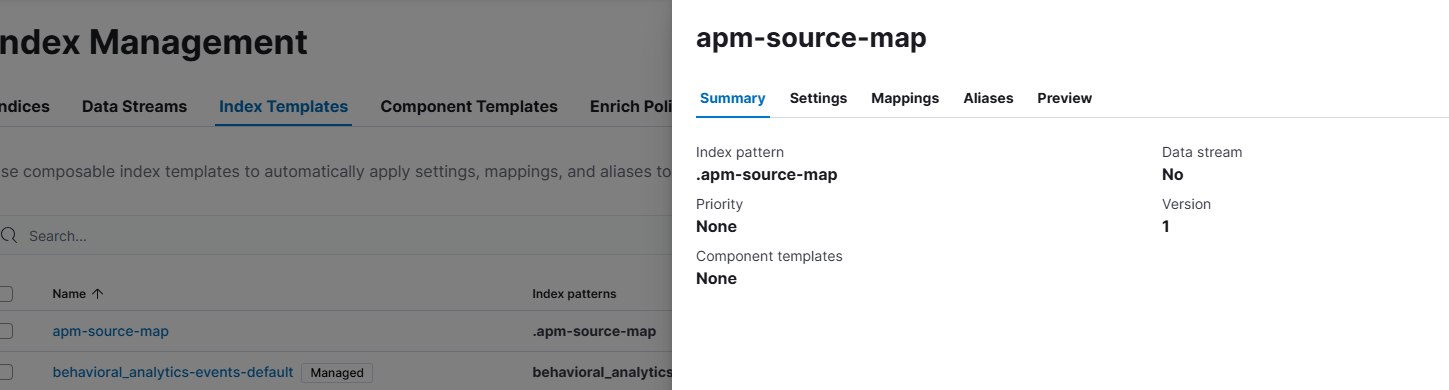
There will different indexes like IIS will have different index and mysql have different index

Index prefix is always going to be the same and suffix is going to change due to the fact we are going to apply rolling index through defining templates and setting for the index; the method is called roll-over index. We will have to have ILM policy attached to it too as well as per the data-lake techniques and method

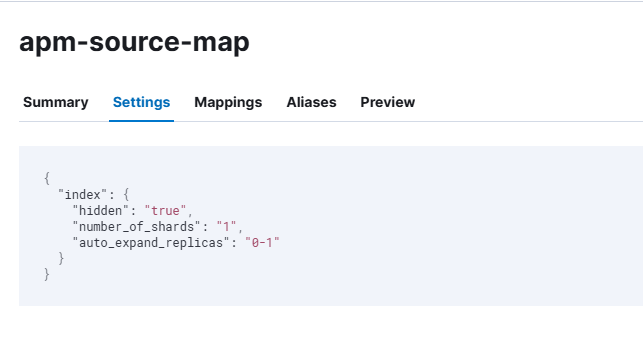
## Index Template

For each index, we can define the index template in the Index Template under Index management



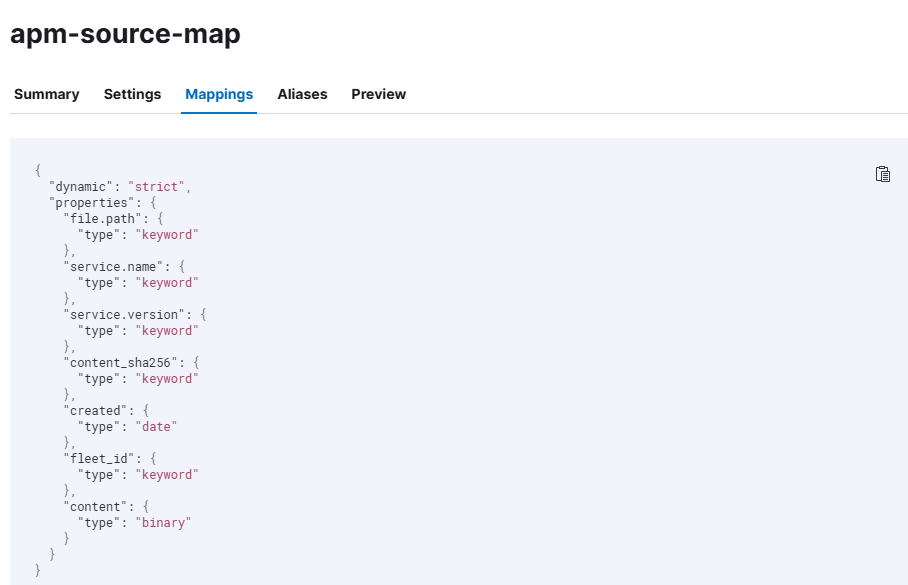


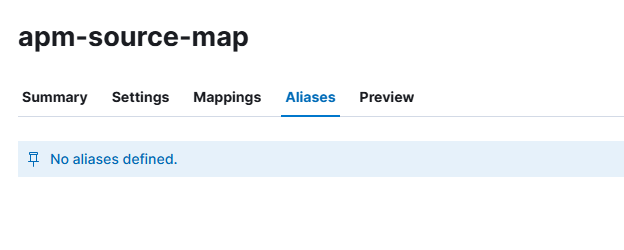
The settings are as follows

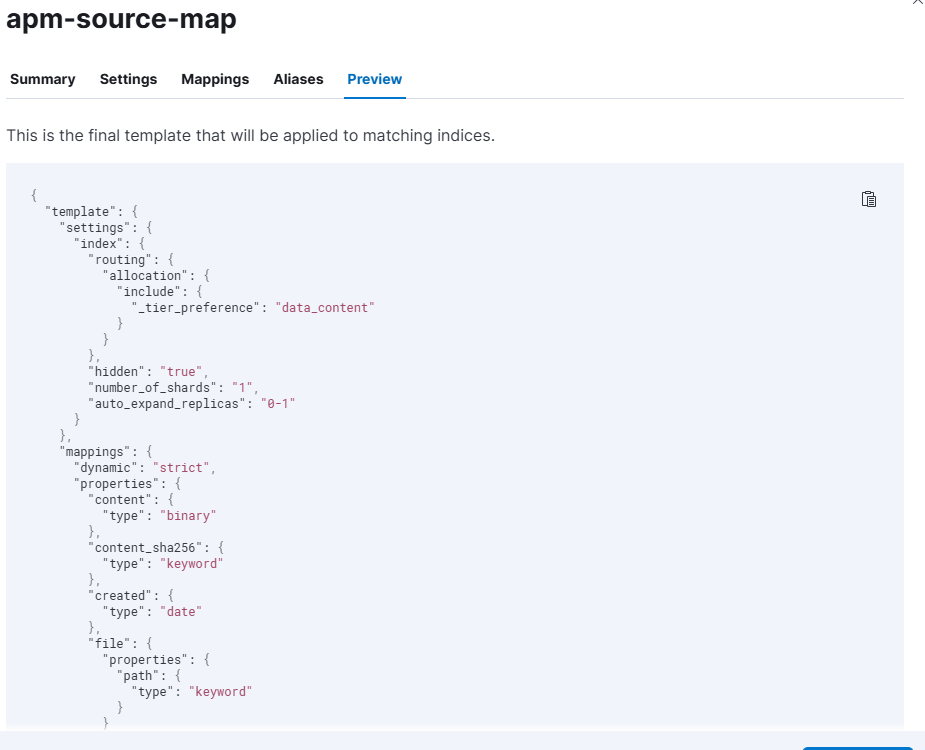


any index that have this index template applied, it will be mapped according to mappings below:

This is a data type mapping, meaning which field is going to contain what data type

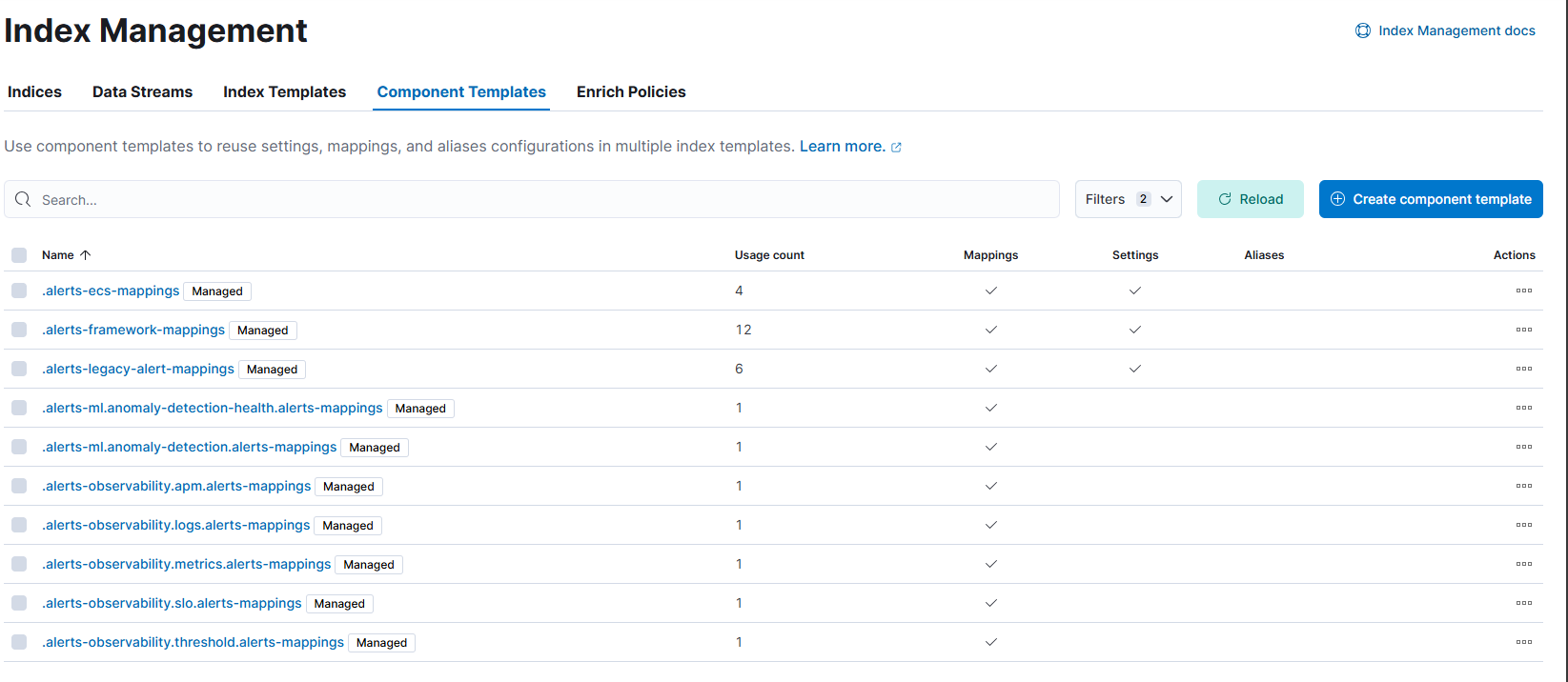






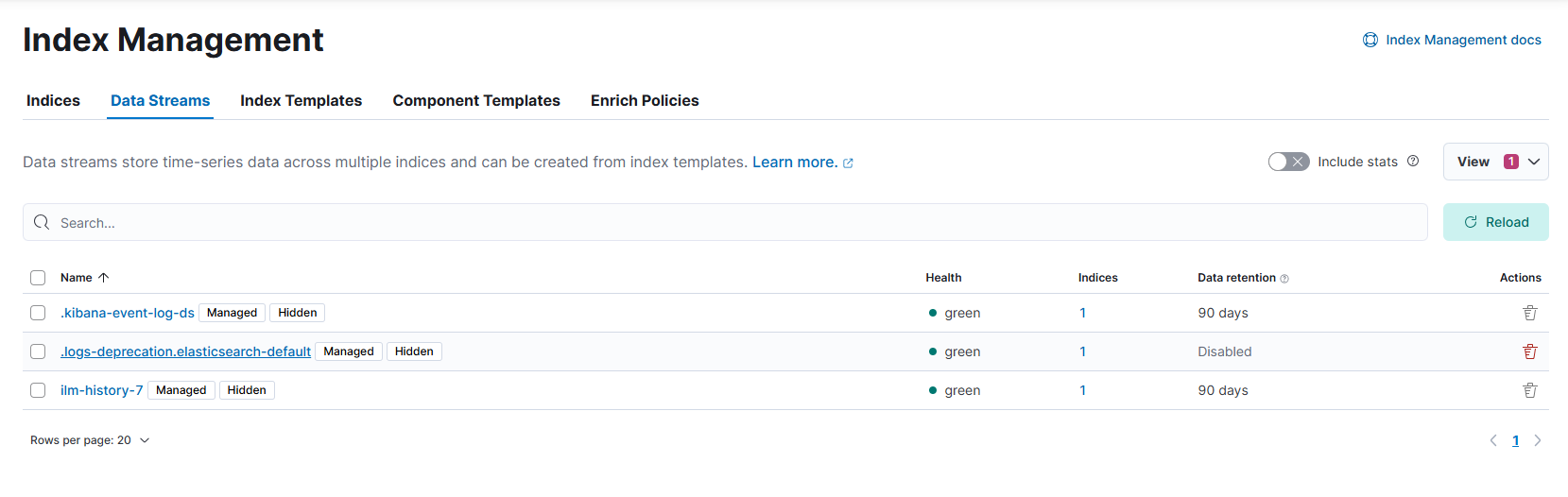
|  |
| --- |
| {  "template": {  "settings": {  "index": {  "routing": {  "allocation": {  "include": {  "\_tier\_preference": "data\_content"  }  }  },  "hidden": "true",  "number\_of\_shards": "1",  "auto\_expand\_replicas": "0-1"  }  },  "mappings": {  "dynamic": "strict",  "properties": {  "content": {  "type": "binary"  },  "content\_sha256": {  "type": "keyword"  },  "created": {  "type": "date"  },  "file": {  "properties": {  "path": {  "type": "keyword"  }  }  },  "fleet\_id": {  "type": "keyword"  },  "service": {  "properties": {  "name": {  "type": "keyword"  },  "version": {  "type": "keyword"  }  }  }  }  },  "aliases": {}  }  } |

## Component Template



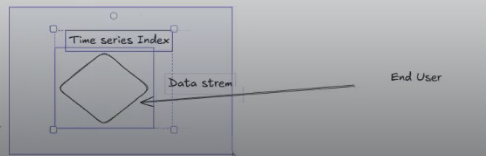
We are going to understand the difference between the index template and component template later.

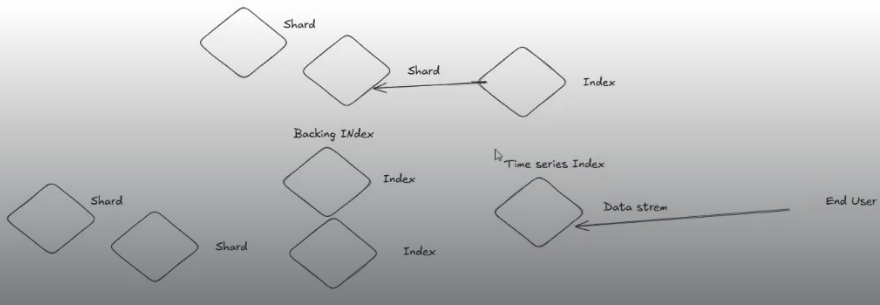
## Data Stream and Indices



Datasteam and indices are same thing but data stream is the real time logging with time-series index (real time stream) containing information second by second or minute by minute.

End user decides whether the data will go to the data stream or the index





If you notice the there is backing index in Data Stream but there is no Backing index in the Index itself. For Index we directly index and then shard which is located on server or some filesystem where the data is stored.

Data Stream is going to be the collection of multiple backing index, meaning that it is managing the indexes at the time series level; it will create the multiple indexes automatically, we only have to define the data stream only. Why matters for the visualization of the timeseries data, it manages the indices and we don’t manage the indices.

For our data retrieval, we directly write the data on the index, which will be managed by us.

### Summary: Data stream vs Index

* Time series will be managed by the data stream, it will take care of managing and writing to the backing index and this backing index will have a shard.
* Data stream is the collection of the backing index. Both are going to contain the data only which will be managed by the end user.
* Data stream manages index itself but the index we manage it

**🔍 Indices vs. Data Streams**

**📁 1. Index:**

An **index** in Elasticsearch is like a **container** for documents (your data).

* You can send data **directly to an index**.
* Typically used for **structured data** or **logs**, e.g., web-logs-2025.
* You manage **index lifecycle** manually or via ILM (Index Lifecycle Management).
* Real-time ingestion: Yes, logs can be sent to an index in real time.

✅ **Use indices when**:

* You have **one-off datasets** or don’t need rollover/index rotation.
* You manually manage retention or sizes.
* You don’t need the auto-managed time-based data flow.

**🌊 2. Data Stream:**

A **data stream** is a **higher-level abstraction** designed **specifically for time-series data**, like logs or metrics.

* It **automatically creates backing indices** (e.g., .ds-logs-000001, .ds-logs-000002, etc.).
* You **don’t write directly to indices**—you write to the **data stream alias**, like logs-system.
* Elasticsearch handles **index rollovers**, retention, and ILM policies under the hood.
* Optimized for **real-time, append-only data**.

✅ **Use data streams when**:

* You’re working with **logs, metrics, or time-based data**.
* You want **automated rollover, retention**, and **index management**.
* You want cleaner **ingestion pipelines**.

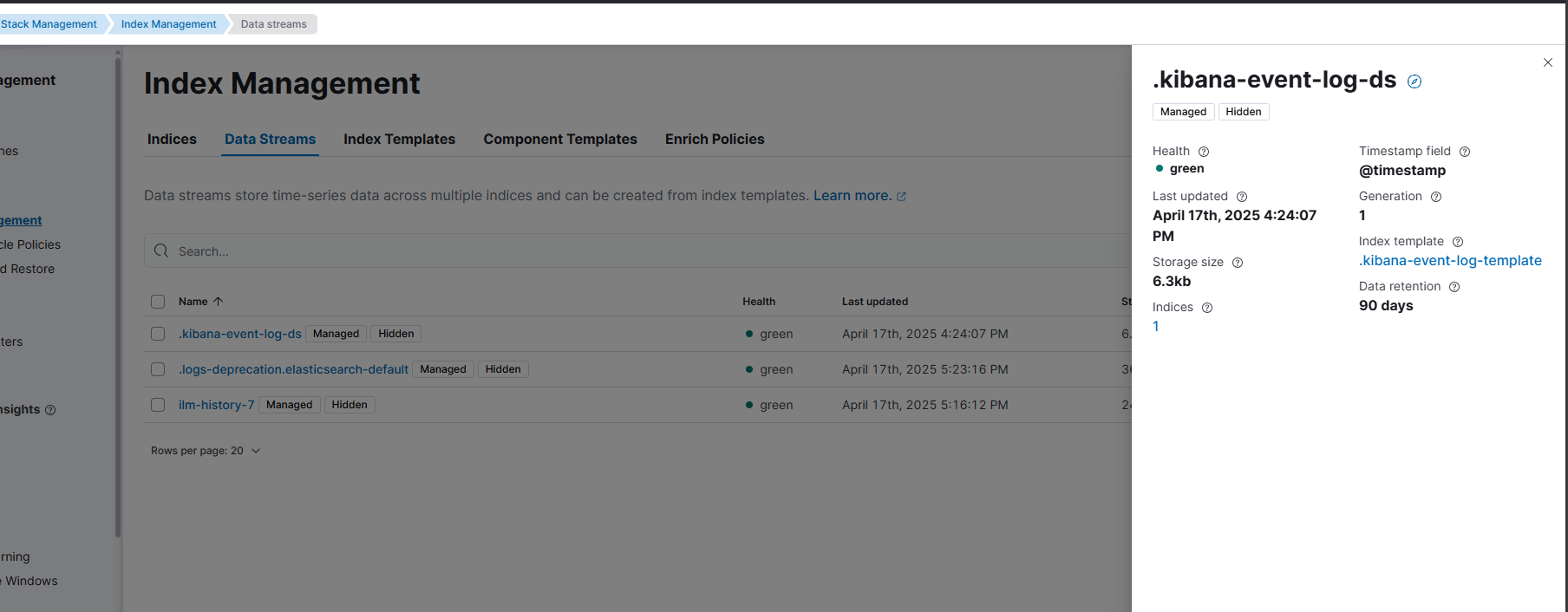
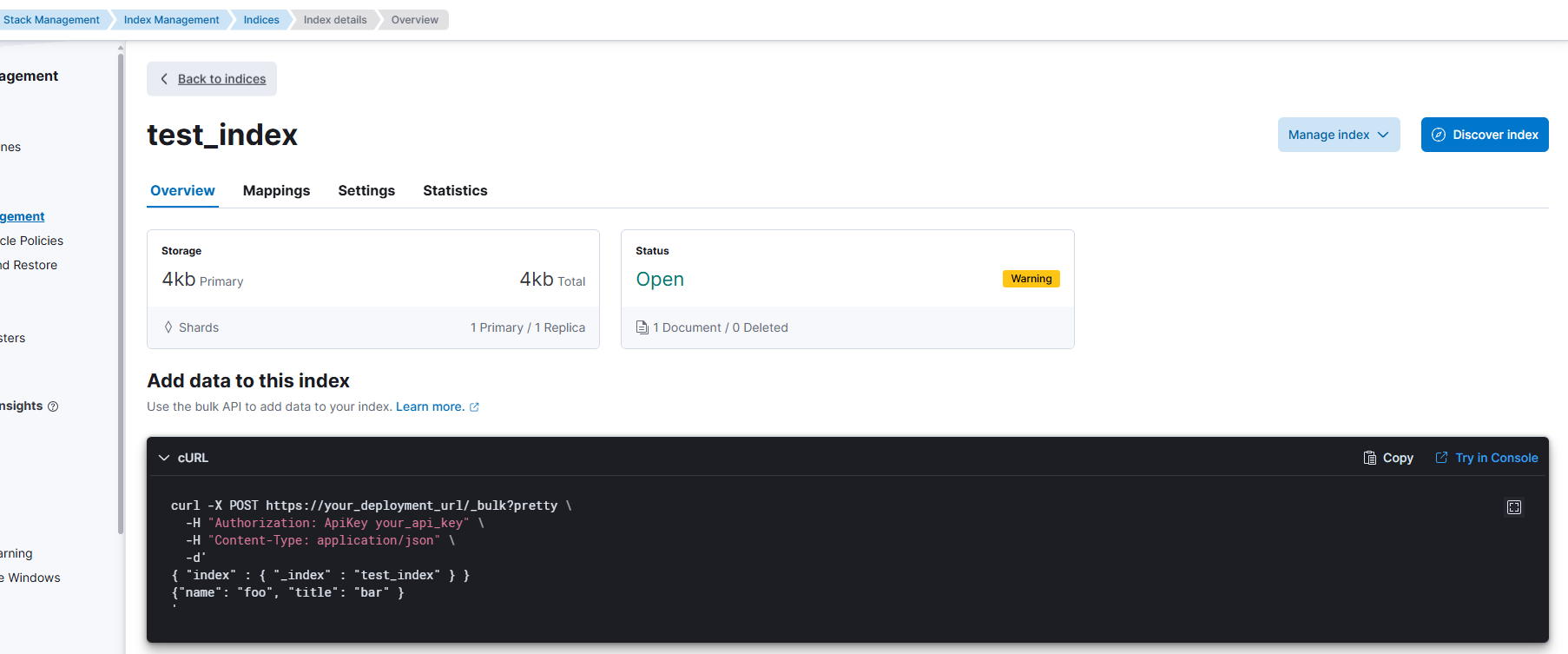
### 🆚 Summary Table:

| **Feature** | **Index** | **Data Stream** |
| --- | --- | --- |
| Real-time ingestion | ✅ Yes | ✅ Yes |
| Target of writes | Direct to index | Write to stream alias (e.g., logs-\*) |
| Rollovers | Manual or via ILM | Automatic |
| Backed by | One index | Multiple indices (hidden) |
| Ideal for | General-purpose storage | Time-based data (logs, metrics) |

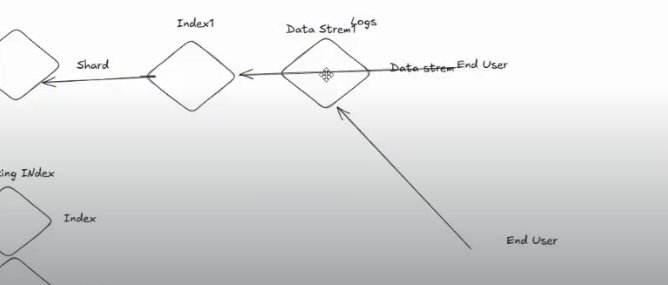
**⚠️ Final Note:**

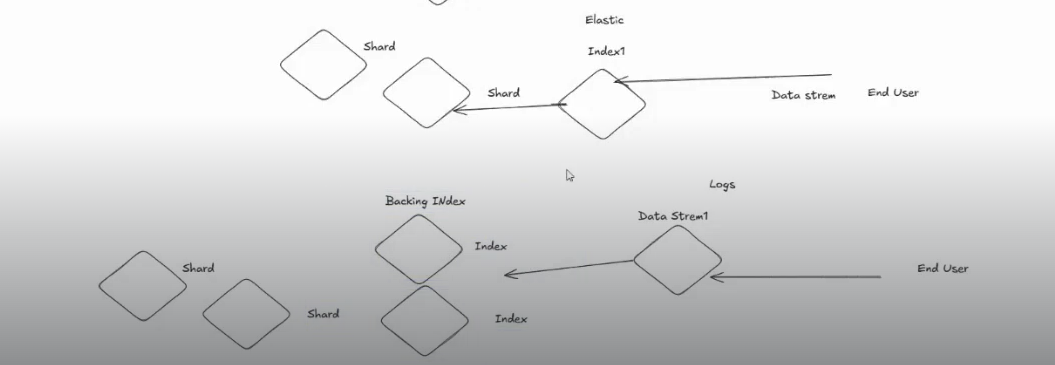
Yes, both can **receive logs in real time**, but **data streams handle the storage lifecycle smarter** — especially for time-based or high-volume data.

### Some more explanation

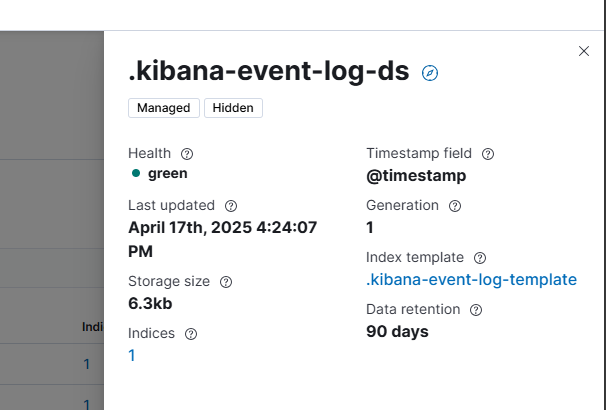


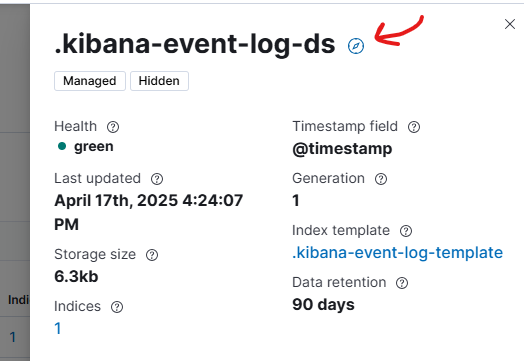
If you were to place the datastream before index, it will become a datastream structure but still have to do the backing index



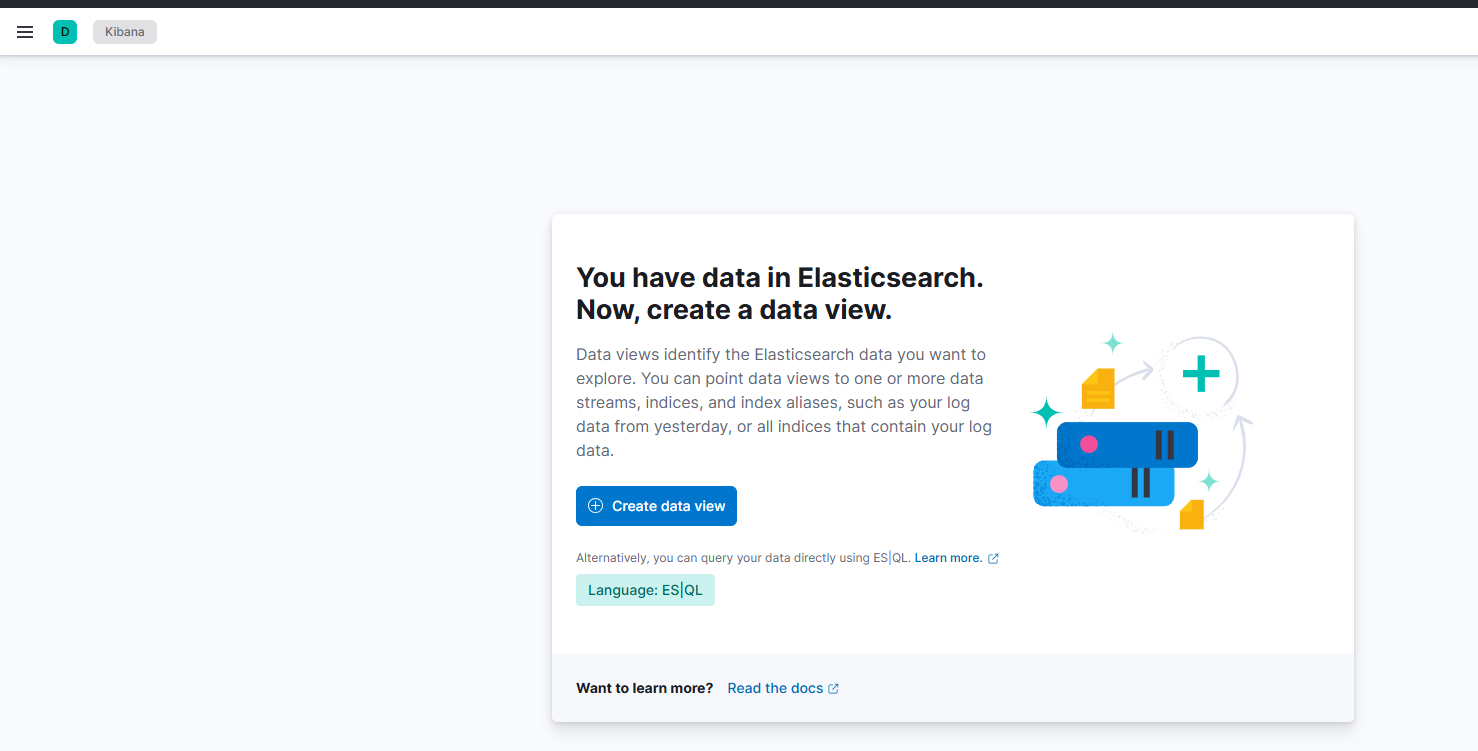


In our case .kibana-event-log-ds is a datastream

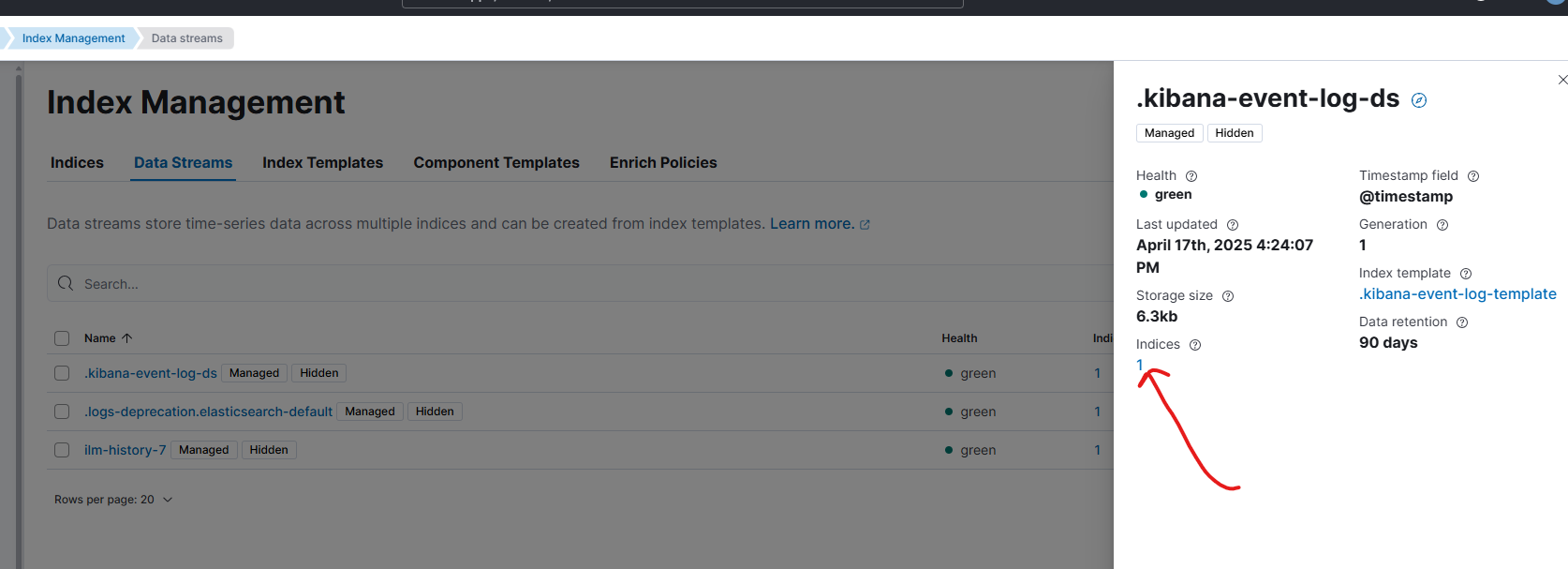


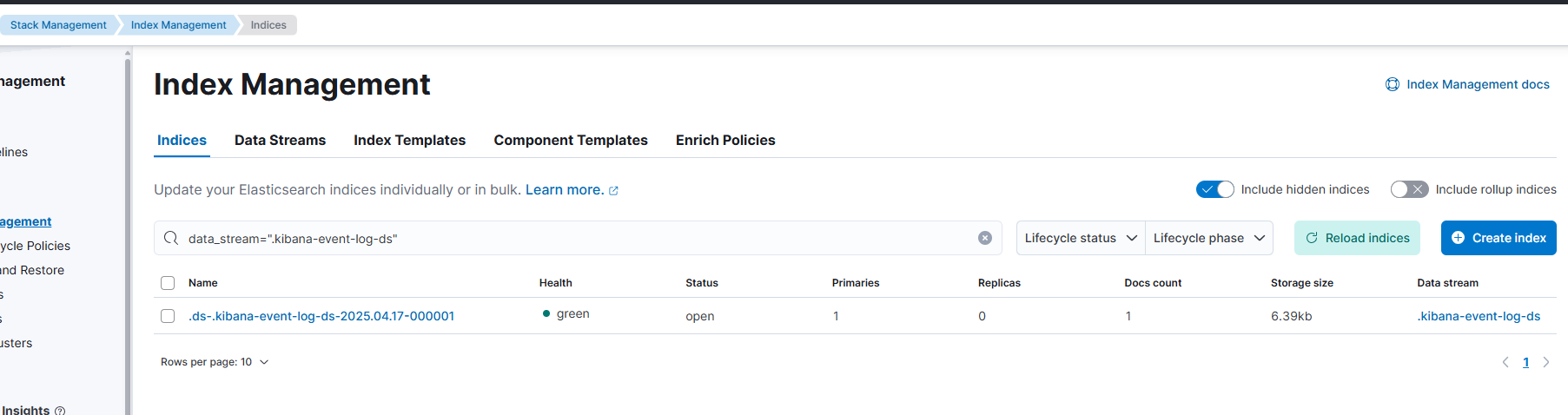


And the backing index we are not able to see and not able to delete

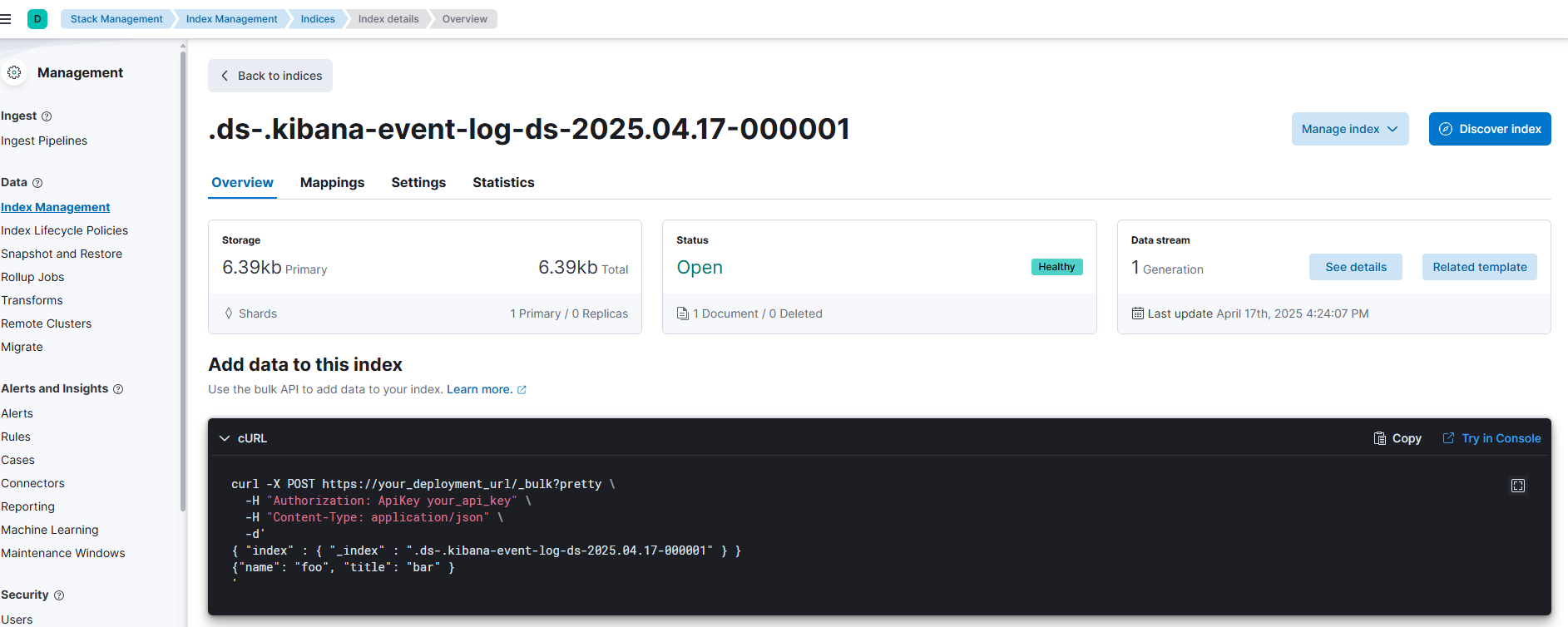


If you click on indices, you will be able to see the datastream index





This is the index which was created by the **.kibana-event-log-ds** that we previously saw.

for efficient time-series data management should be utilized. (we will do lab on this later)

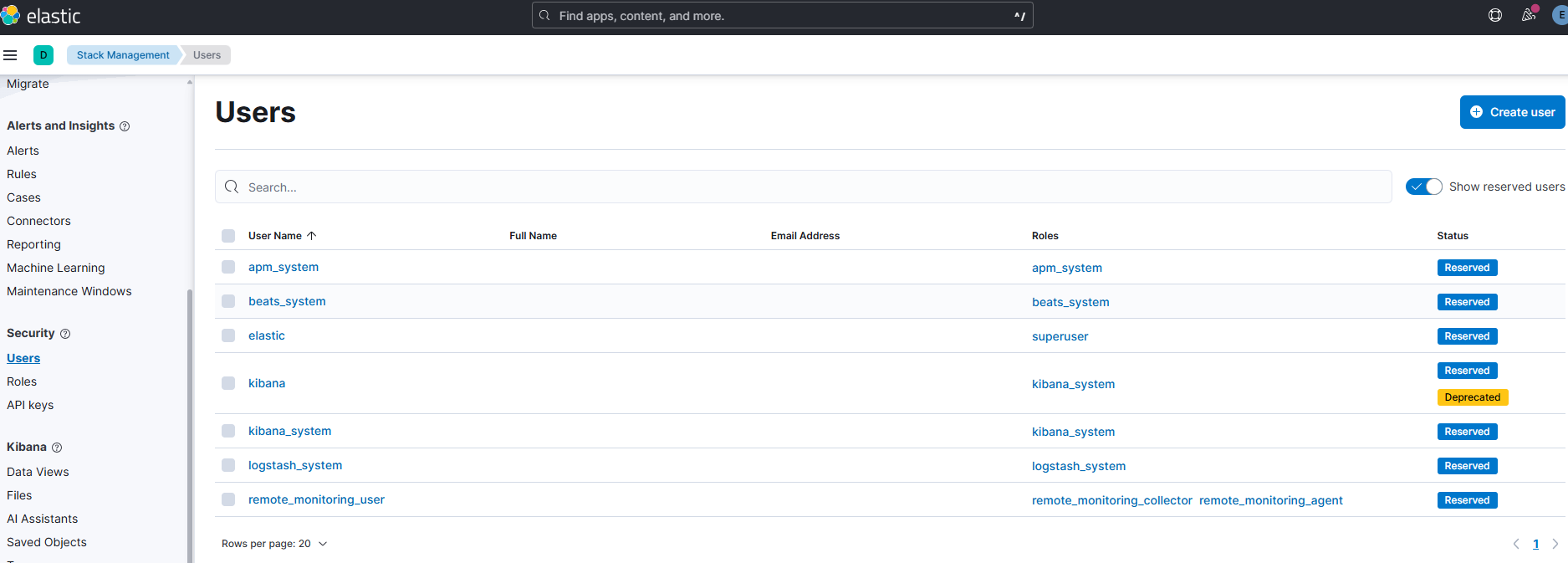
## Security

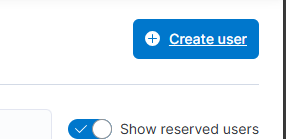
### Users

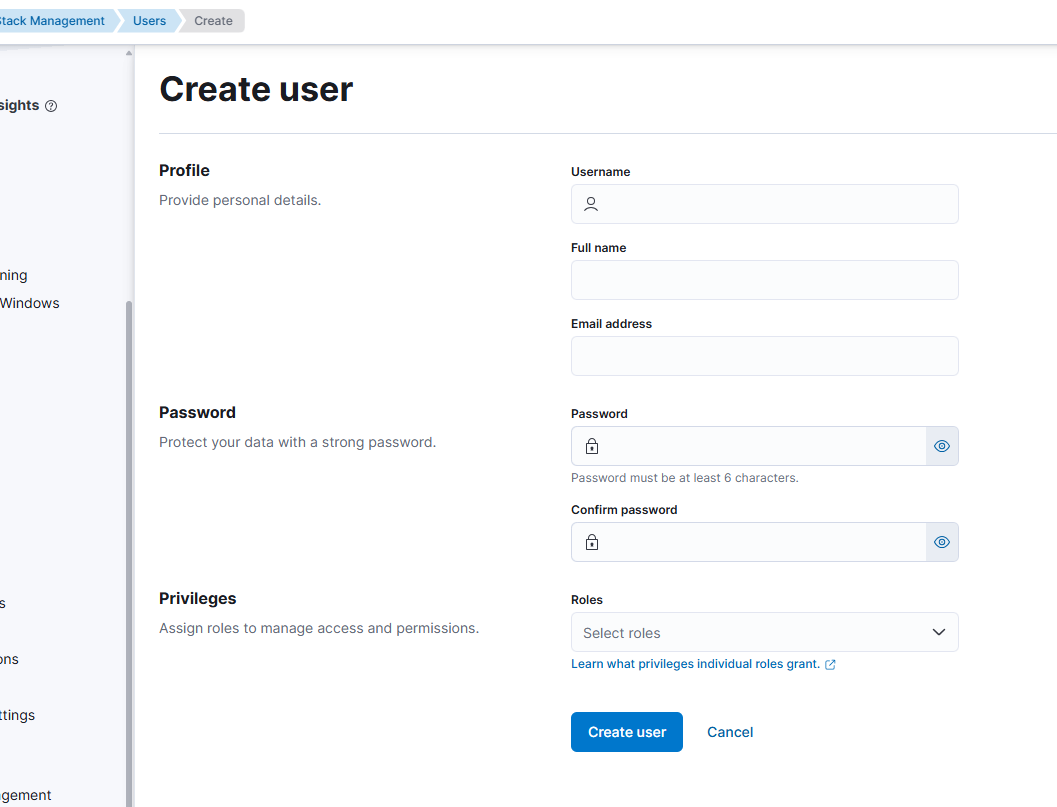
If you were not logged in as the super-user, you will not see a lot of options. You should learn user management using kibana as well

We logged in as kibana\_system but how is kibana fetching the data from elasticsearch is throught kibana\_system. If you want to create more user there is one method of using API which we used previously or through clicking on create user

Click stack management > under security click on Users

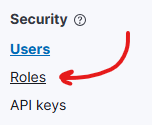




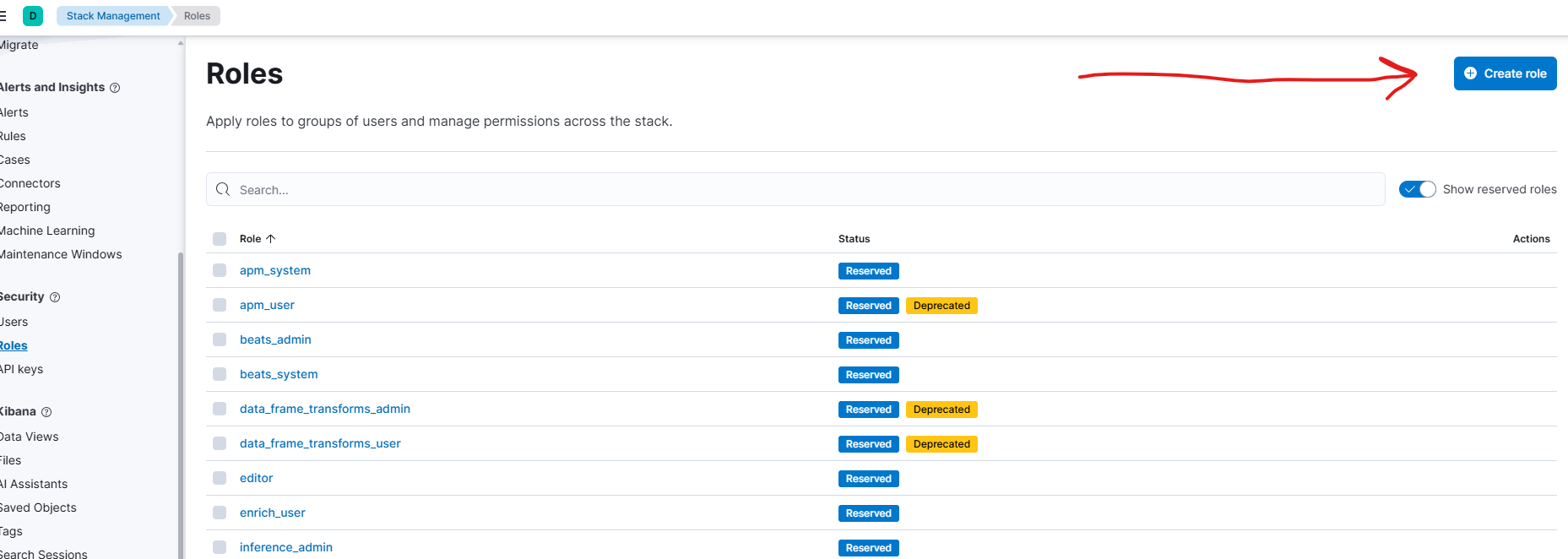


### Roles

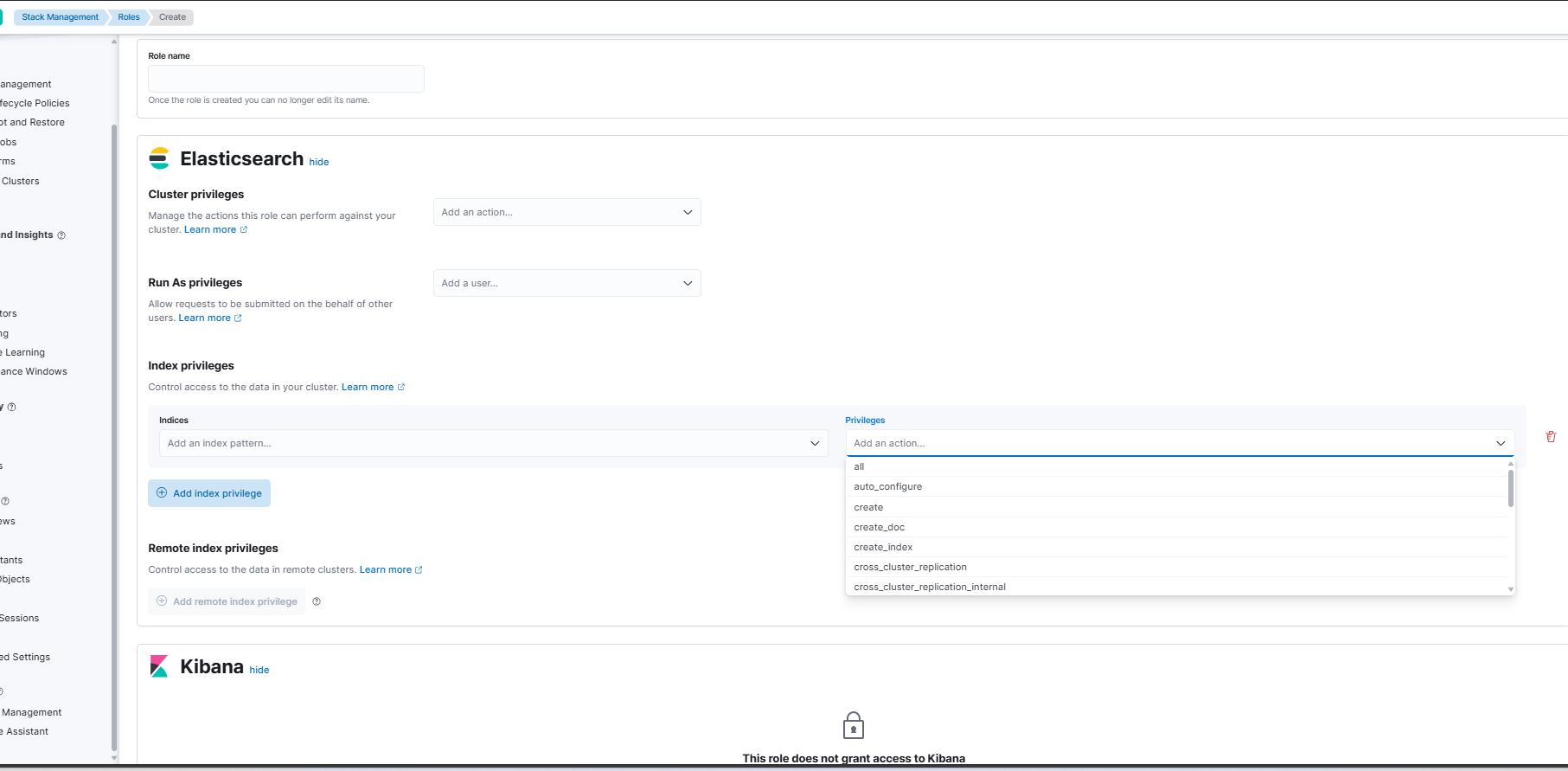
You can create Roles as well click on roles under security



Click on create roles



IMPORTANT to discover this: You can give privileges from this section



What we covered so far.

We hosted our elasticsearch on a single cluster, we assigned self-signed ssl certificates to it.

And then we opened a port 9200 and we installed kibana, we installed elastic certificate to kibana.

Next we will generate the certificate for kibana as well, to access kibana from certificate also; that is pending.

We went through the walk through of kibana dashboard in this document.