**Step 1: Create an Index Template**

Index templates allow you to define settings, mappings, and aliases for indices that match a certain pattern.

Run this command in **Kibana Dev Tools**:

PUT \_index\_template/my\_template

{

"index\_patterns": ["logs-\*"],

"template": {

"settings": {

"number\_of\_shards": 1,

"number\_of\_replicas": 1

},

"mappings": {

"properties": {

"timestamp": {

"type": "date"

},

"message": {

"type": "text"

},

"status\_code": {

"type": "integer"

}

}

}

}

}

**Explanation:**

* The template applies to indices matching **logs-**\* (e.g., logs-2024-03, logs-web, etc.).
* It sets **shards** and **replicas** for better performance.
* Defines **mappings** for fields:
  + timestamp as **date**.
  + message as **text**.
  + status\_code as **integer**.

**Step 2: Create an Index Matching the Template**

Once the template is created, any index that matches the pattern **logs-**\* will inherit its settings.

Example:

PUT logs-2024-03

This creates an index **logs-2024-03** using the **my\_template** settings.

**Step 3: Insert a Document**

Now, let's add a document to the index:

POST logs-2024-03/\_doc/1

{

"timestamp": "2025-03-04T12:00:00",

"message": "User logged in successfully",

"status\_code": 200

}

* This inserts a log entry with a timestamp, message, and status code.

**Step 4: Verify the Document**

To check if the document is indexed, run:

GET logs-2024-03/\_search

It will return the inserted document.

**1. Create an Index Template**

Index templates help define **settings**, **mappings**, and **aliases** for indices.

Run this in **Kibana Dev Tools**:

PUT \_index\_template/my\_index\_template

{

"index\_patterns": ["my-index-\*"],

"template": {

"settings": {

"number\_of\_shards": 1,

"number\_of\_replicas": 1

},

"mappings": {

"properties": {

"timestamp": {

"type": "date"

},

"user": {

"type": "keyword"

},

"message": {

"type": "text"

},

"status": {

"type": "integer"

}

}

}

}

}

**Explanation:**

* This template applies to indices matching **my-index-**\* (e.g., my-index-2025-03).
* It sets **shards** and **replicas** for performance tuning.
* Defines **mappings** for fields:
  + timestamp → **date** type
  + user → **keyword** (exact search)
  + message → **text** (full-text search)
  + status → **integer**

**2. Create an Index (Using the Template)**

When you create an index matching **my-index-**\*, it will **automatically use the template**.

PUT my-index-2025-03

This creates **my-index-2025-03** with the **my\_index\_template** settings.

**3. Insert a Document into the Index**

Now, let's add a document to the index:

POST my-index-2025-03/\_doc/1

{

"timestamp": "2025-03-04T12:30:00",

"user": "john\_doe",

"message": "User logged in",

"status": 200

}

* This **stores a document** with a timestamp, user, message, and status.

**4. Retrieve the Document**

To **fetch all documents** from the index:

GET my-index-2025-03/\_search

This will return the inserted document.

**5. Verify the Index Mapping**

Check if the index **correctly applied the template mappings**:

GET my-index-2025-03/\_mapping

It will show the **field types** (e.g., timestamp is date, user is keyword).

**✅ Key Learning Points for Students**

1. **Index Templates** ensure consistency across multiple indices.
2. **Index Creation** inherits settings/mappings from templates.
3. **Document Insertion** follows the defined mappings.
4. **Querying Data** retrieves documents efficiently.