# 

# Detailed Notes: Index Templates and Elastic Common Schema (ECS)

## Introduction

* - Kibana has been set up, and now we are ready to import test data.
* - The first step involves adding two \*\*index templates\*\*.

## What Are Index Templates?

* - \*\*Definition\*\*: Automatically apply **index settings** and **mappings** when a new Elasticsearch index is created, based on a defined name pattern.
* - \*\*Example\*\*:

- A query results in the creation of a new index.

- If an index template matches the index name, the provided settings and mappings are automatically applied.

## Purpose of Index Templates

* - To ensure documents are mapped and indexed according to the \*\*Elastic Common Schema (ECS)\*\*.
* - \*\*Elastic Common Schema (ECS)\*\*:

- A specification defining field names and their mappings.

- Ensures consistency across different datasets.

## Example: ECS in HTTP Access Logs

1. 1. \*\*Before ECS\*\*:

- Field names varied between different web servers (e.g., nginx vs Apache).

- This caused inconvenience when working with data in Kibana:

- Changing web servers required reindexing logs and reconfiguring Kibana.

1. 2. \*\*After ECS\*\*:

- ECS standardizes field names and mappings for common fields.

- Example:

- The URL of an HTTP request uses the same field name regardless of the web server.

- The field `@timestamp` is used for the time of an event across all technologies.

- \*\*Advantage\*\*:

- Consistency and ease of working with data, regardless of the underlying technology.

## Adding Index Templates

1. 1. \*\*Steps to Add Index Templates\*\*:

- Copy large queries from a GitHub repository provided with the course.

- Use Kibana’s \*\*Console Tool\*\* (introduced in the previous lecture) to send queries.

1. 2. \*\*Access Logs Dataset\*\*:

- The index template matches indices starting with `access-logs` followed by a date (e.g., `access-logs-YYYY-MM`).

- For large datasets:

- One index per day is suggested.

- In this course, one index per month is sufficient.

3. \*\*Orders Dataset\*\*:

- Add another index template for the orders dataset using the same process.

## How to Use Kibana for Index Templates

1. 1. Open the \*\*Console Tool\*\* in Kibana.
2. 2. Paste the copied query into the editor.

3. Run the query to apply the index template.

## Importance of ECS and Index Templates

* - \*\*ECS\*\*:

- Provides standardized field names and mappings.

- Useful for indexing documents and configuring Kibana.

* - \*\*Index Templates\*\*:

- Automate the application of consistent mappings and settings.

- Reduce manual effort and ensure compatibility with ECS.

## Conclusion

* - With index templates added, we are ready to index test data into the Elasticsearch cluster.
* - ECS and index templates simplify data management and ensure consistency across datasets.