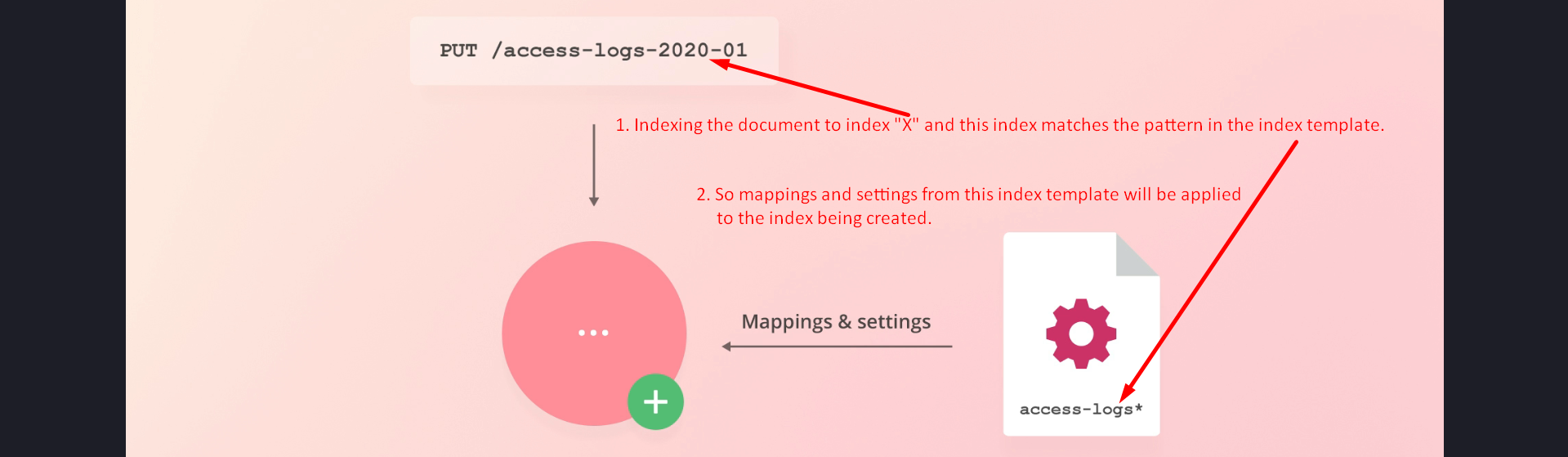
# 

# Adding Index Templates and ECS

## 1. Introduction to Index Templates

Now that Kibana has been set up, we are almost ready to import some test data. We just need to do one thing first: add two **index templates**. Index templates are a way of automatically applying index settings and mappings when a new Elasticsearch index is created — provided that its name matches a pattern that we define.

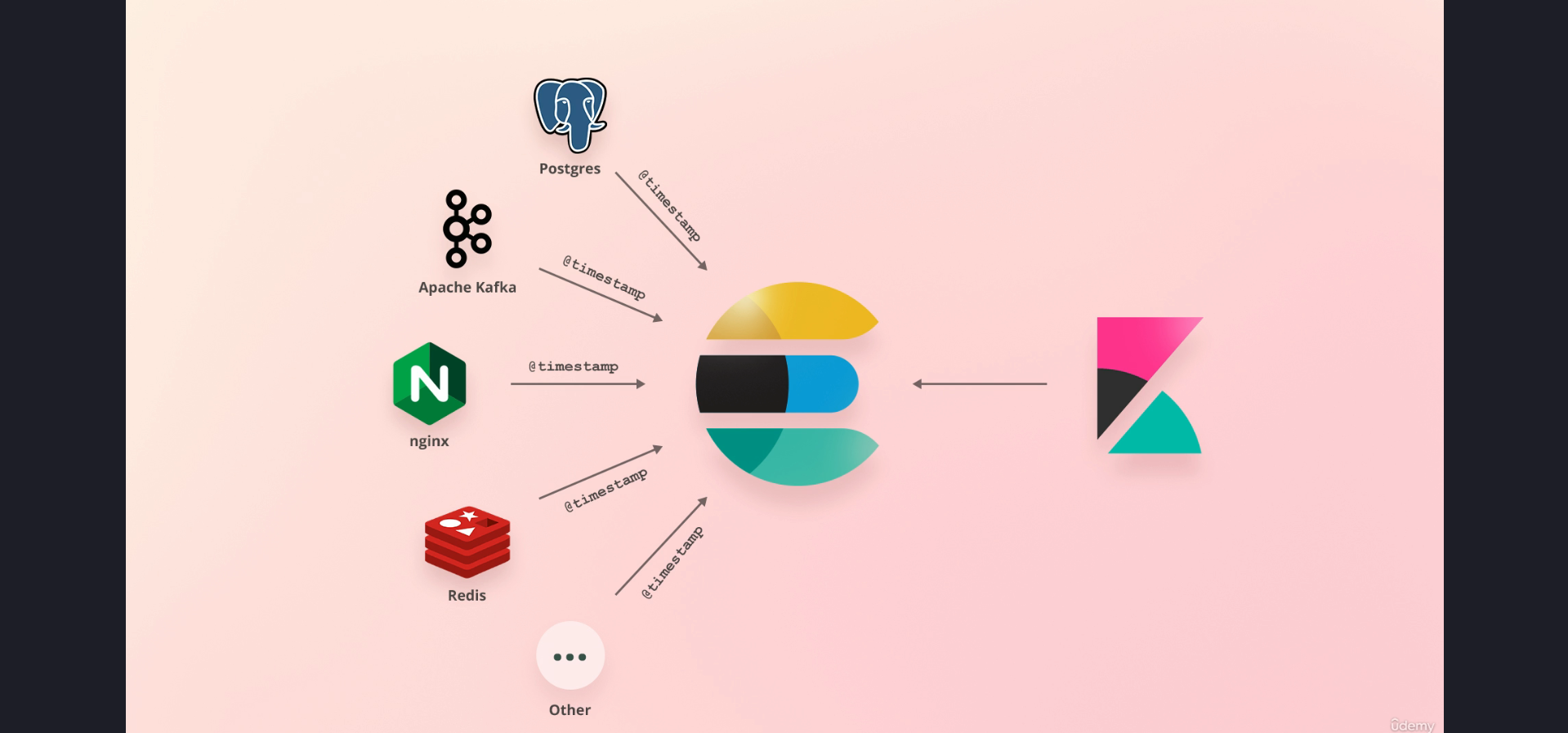
## 2. Example of Index Templates

Consider the example where a new index is created as the result of a query. Since there is an index template with a pattern that matches the name of the index, the mappings and settings provided by the index template are applied. We will use index templates to ensure that our documents are mapped and indexed according to the **Elastic Common Schema (ECS)**, at least in the case of our access logs dataset.  


## 3. Elastic Common Schema (ECS)

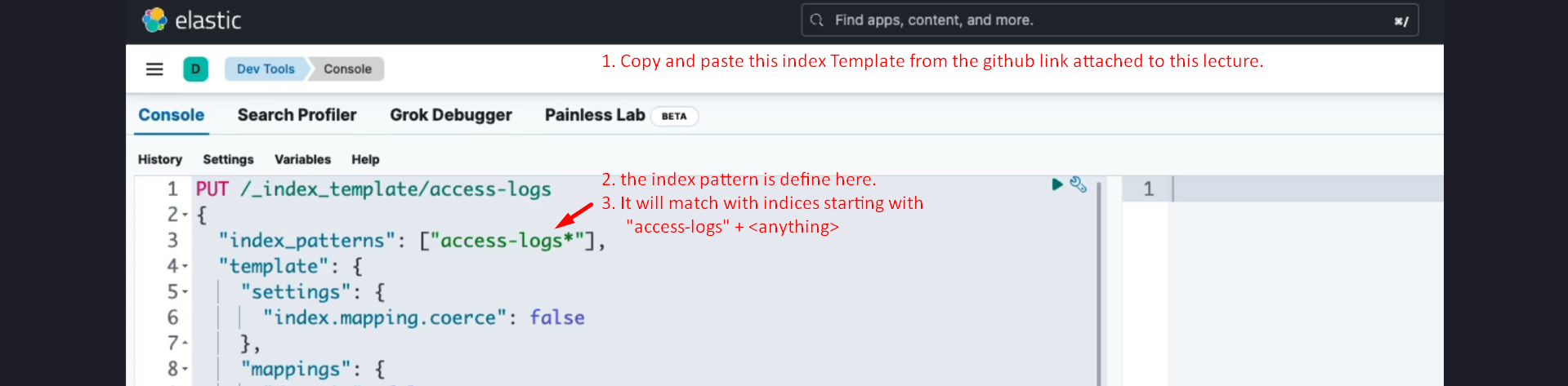
ECS is essentially a specification that defines field names and how they should be mapped. For example, when ingesting HTTP access logs into Elasticsearch, either from nginx or the Apache web server, different field names were traditionally used depending on the web server. This inconsistency made it inconvenient to work with the data within Kibana, as changing the web server required reindexing all access logs and reconfiguring settings within Kibana. ECS solves this problem by introducing standardized field names and mappings for common fields.

For instance, the URL of an HTTP request is the same regardless of the web server used. Similarly, fields common across technologies, such as the time of an event, are standardized. In ECS, the field for event time is named '@timestamp.' This standardization simplifies indexing and querying data.

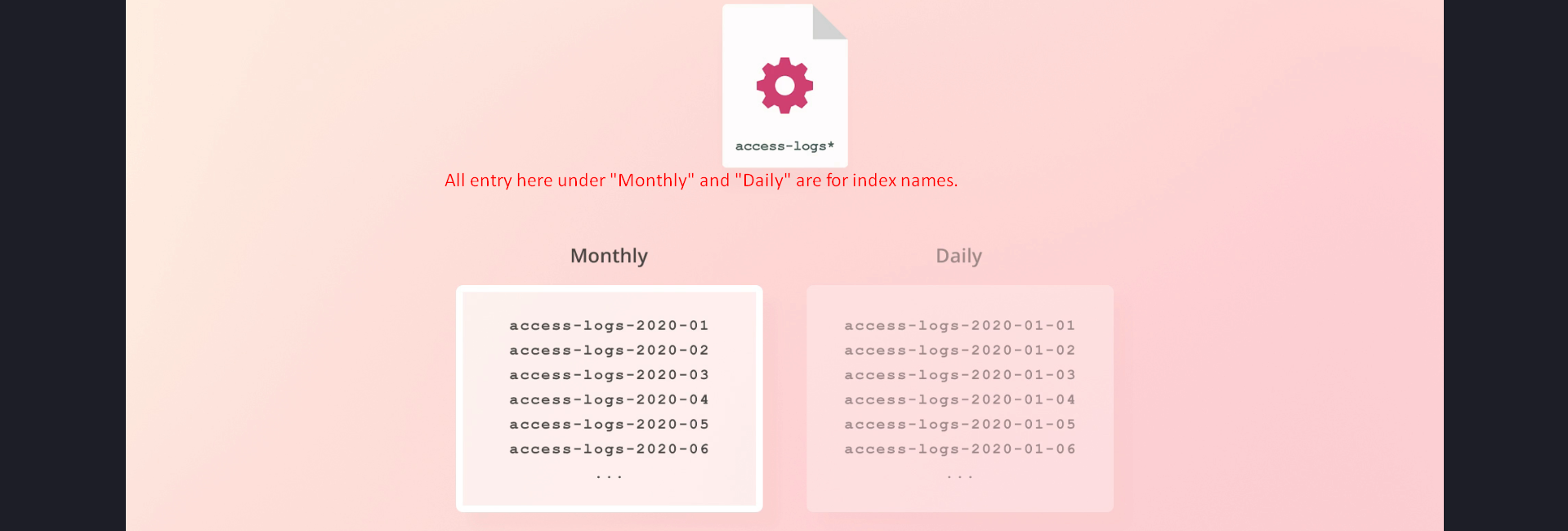


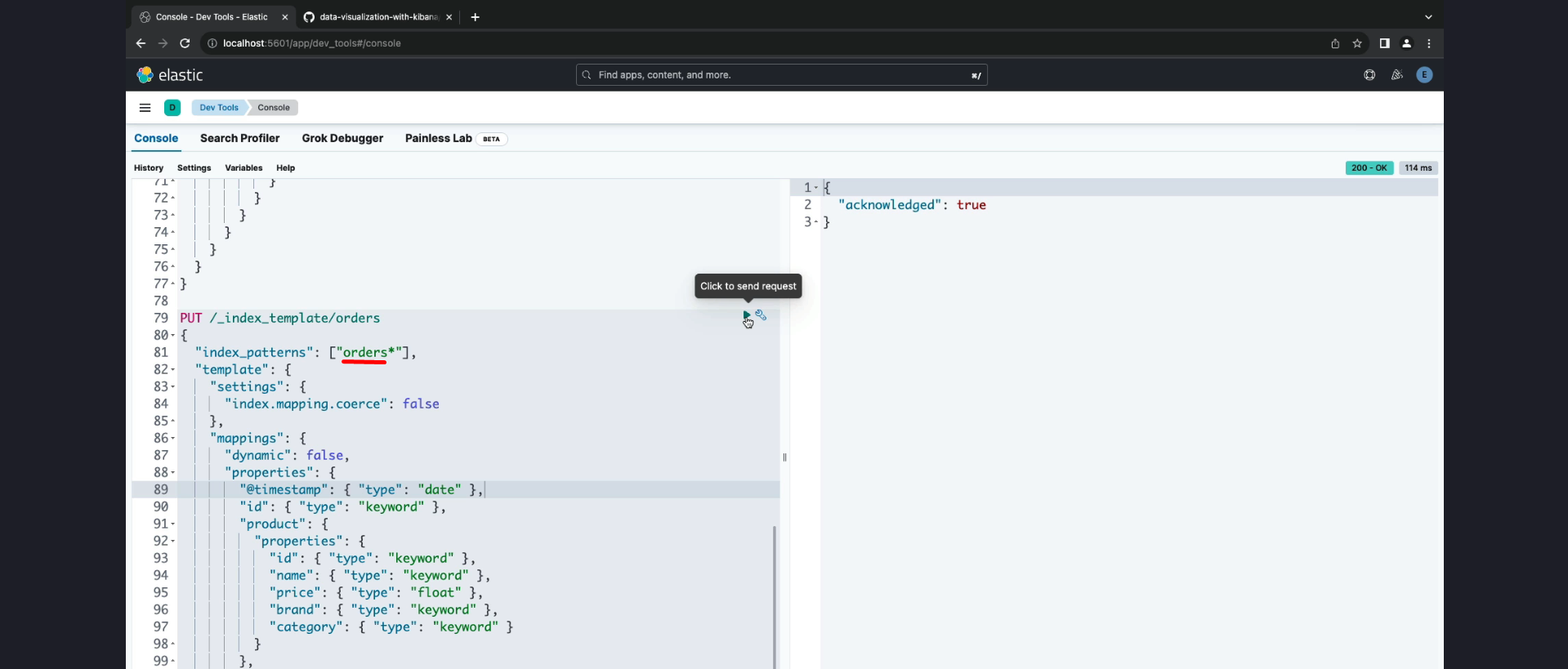
## 4. Adding Index Templates

The queries to add index templates are typically large, so it's convenient to use resources such as a GitHub repository to copy them. For this course, the queries are formatted to be compatible with Kibana's Console tool, which was introduced in the previous lecture.

The first query adds an index template for the access logs dataset. The template matches indices beginning with 'access-logs,' followed by a date.   


This allows for creating indices per day or per month, depending on the amount of data. For this course, we will create one index per month.



After running the query, the index template for the access logs dataset is successfully added. The same process is repeated for the orders dataset, ensuring both datasets have appropriate templates applied.  
  


## 5. Conclusion

With the index templates added, the Elasticsearch cluster is now ready to index test data. These templates ensure that documents are indexed in alignment with ECS standards, making data querying and analysis consistent and efficient.