Taste of Training:

Data Exploration with Kibana and Machine Learning

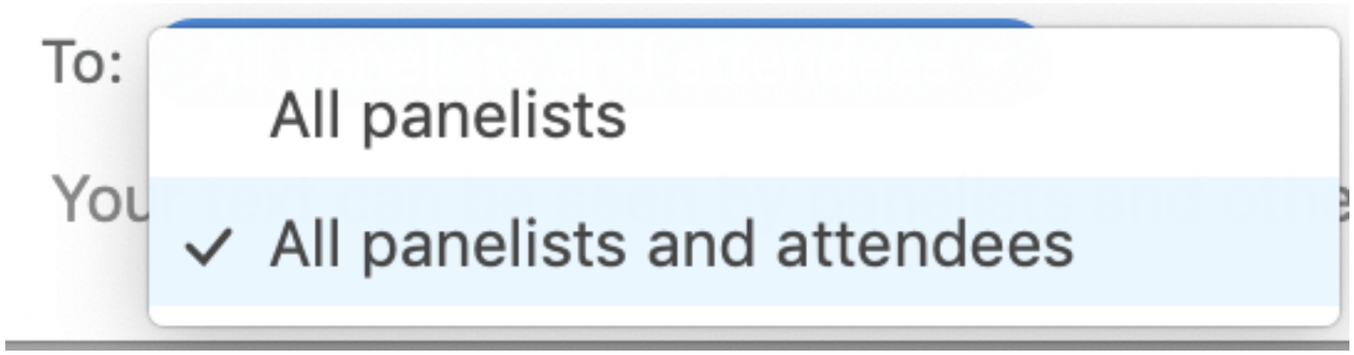
An Elastic Training Course

7.1.0

elastic.co/training

Housekeeping & Logistics

- Attendees are automatically muted when joining Zoom
- Q+A will be at the end of the webinar
- Ask questions for us in the Zoom chat during the webinar
- Chat settings To: All panelists and attendees



- Ask more questions on our discuss forum: discuss.elastic.co
- Recording will be available after the webinar and emailed to all registrants

elastic

Kibana Fundamentals

Lesson 1

Data Visualizer

elastic

Documents

- Elasticsearch is a ***Document Store***
  - Data in Elasticsearch are documents
  - Serialized JSON Object

title	category	date	author_first_name	author_last_name	author_company
Fighting Ebola with Elastic	User Stories		Emily	Mosher	

A row in a table

```
{
  "title": "Fighting Ebola with
Elastic",
  "category": "User Stories",
  "author": {
    "first_name": "Emily",
    "last_name": "Mosher"
  }
}
```

JSON

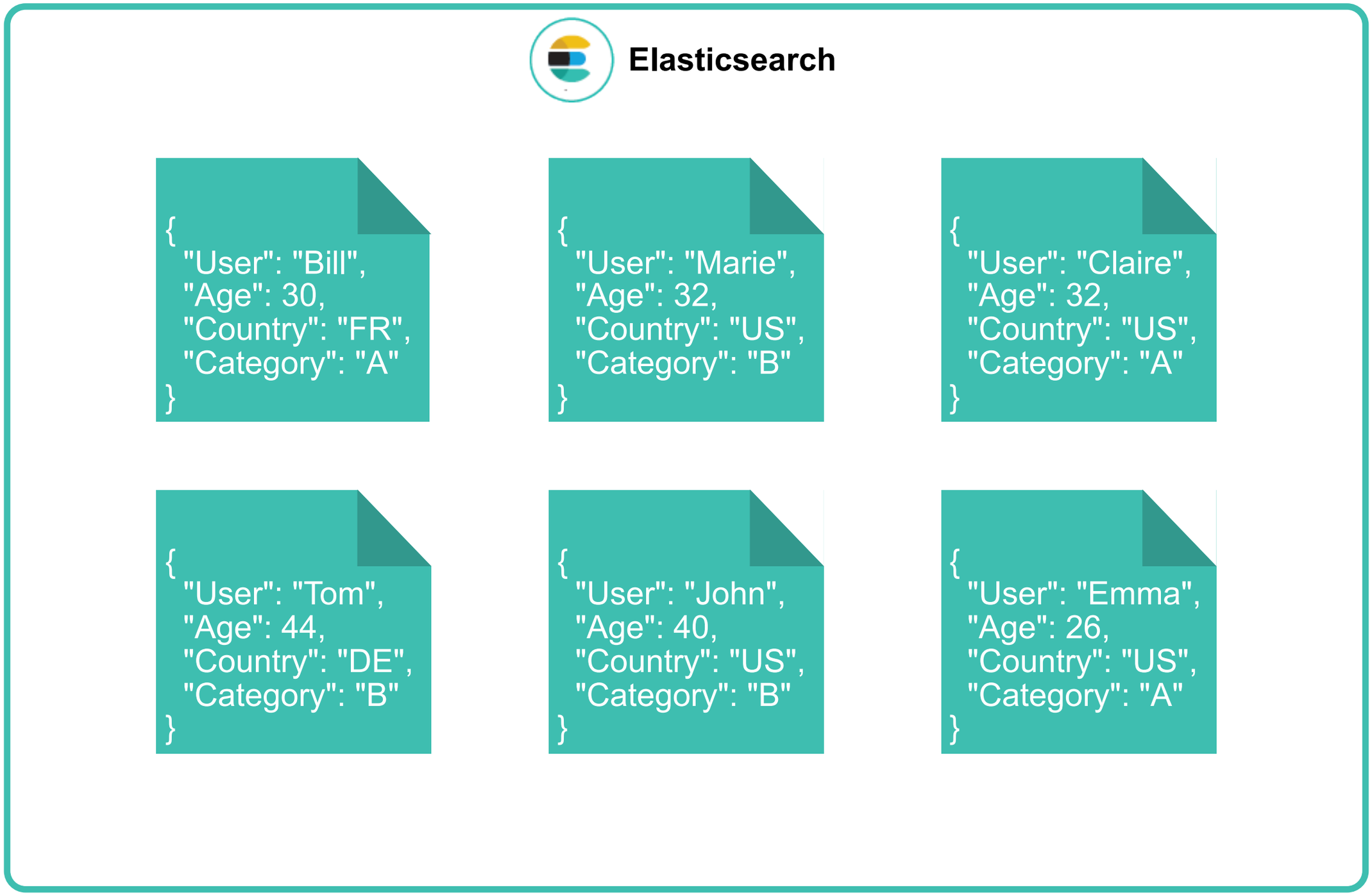
```
<?xml version="1.0" encoding="UTF-8"?>
<root>
   <author>
      <first_name>Emily</first_name>
      <last_name>Mosher</last_name>
   </author>
   <category>User Stories</category>
   <title>Fighting Ebola with Elastic</title>
</root>
```

XML

A Simple Example: Spreadsheet

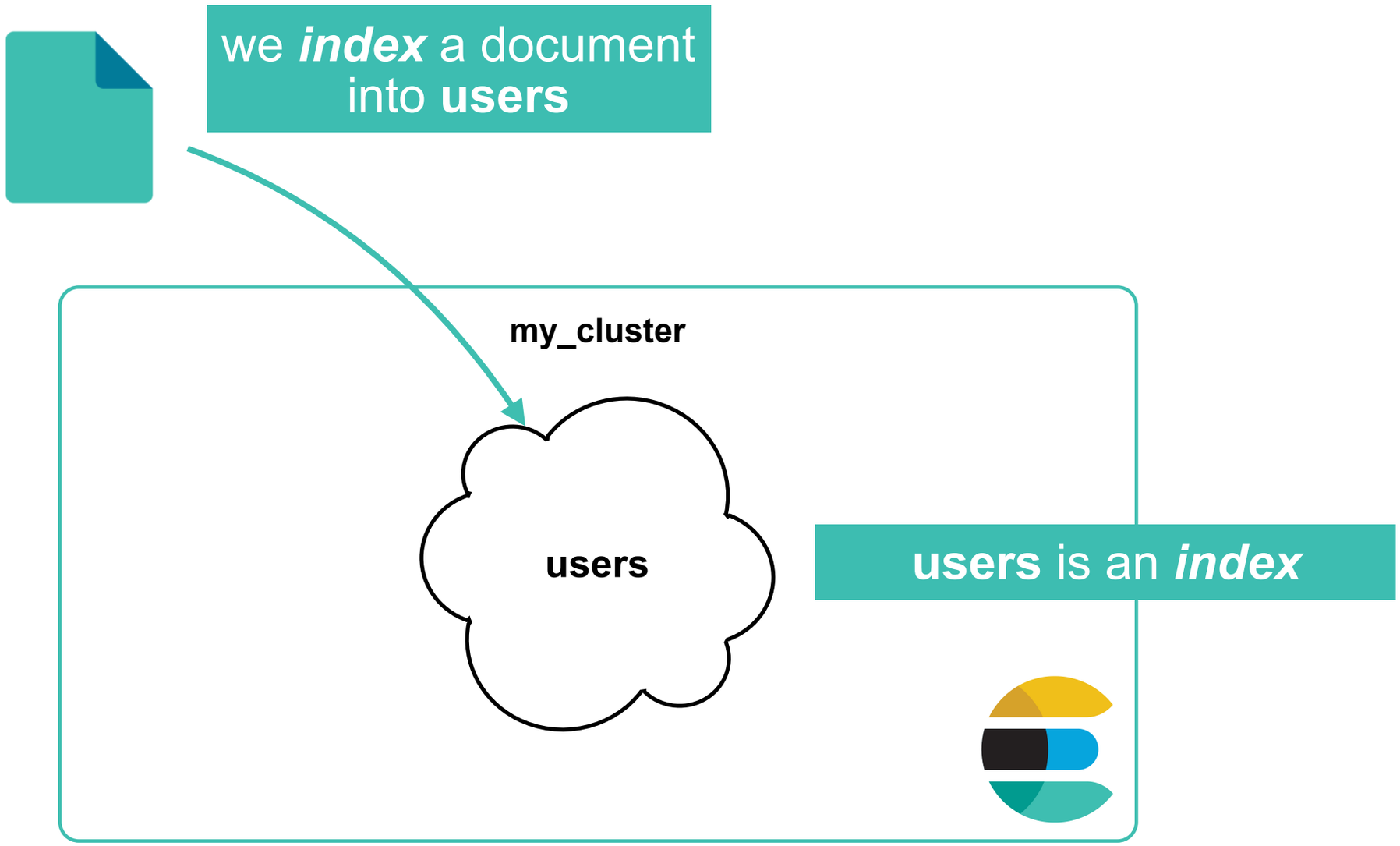
id	user	age	country	category
1	Bill	30	FR	A
2	Marie	32	US	A
3	Claire	32	US	A
4	Tom	44	DE	B
5	John	40	US	B
6	Emma	26	US	B

A Simple Example: Elasticsearch



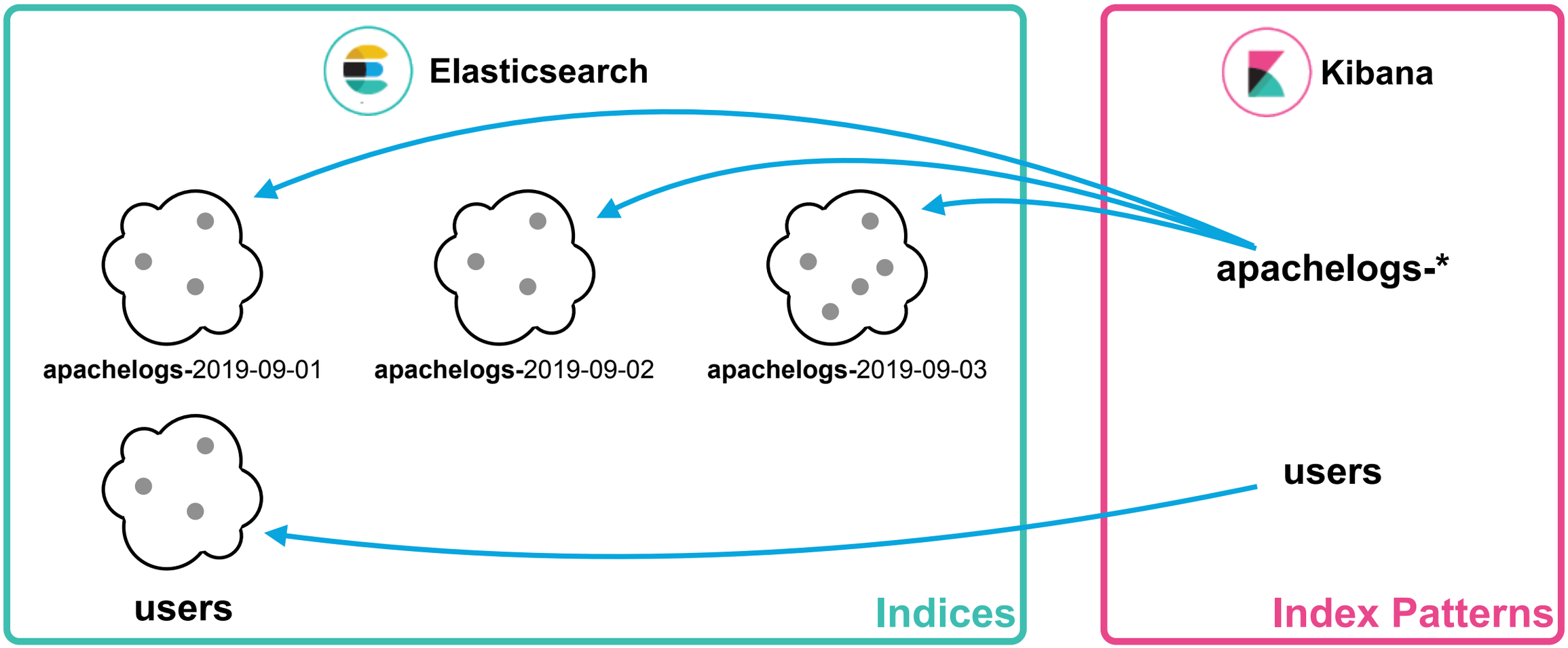
Documents are Indexed into an Index

- In Elasticsearch, a document is ***indexed*** into an ***index***
  - we use **index** as a verb and a noun



Kibana Index Pattern

- Points to one or more Elasticsearch **indices**
- Tells Kibana which data you want to work with



Data Visualizer

- Available with ***Basic*** license
  - Part of Machine Learning time series anomaly detection tool
  - Most Machine Learning tools are available with Platinum license
- Select an ***Index Pattern***
  - Define index patterns in Management > Index Pattern
  - Also can select Saved Searches (from Discover)
- Or Upload a File (marked “experimental”)
  - File size is limited to 100 MB

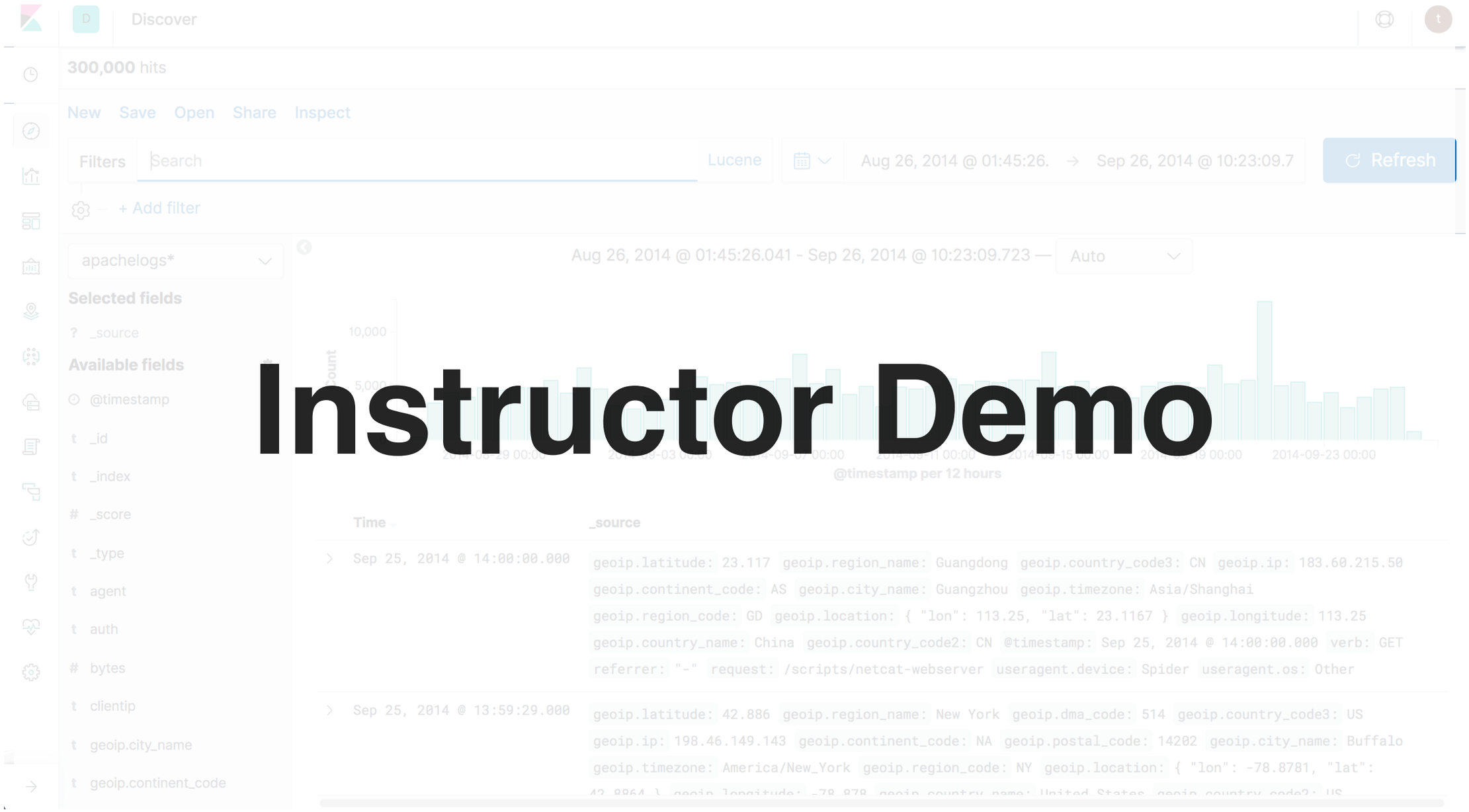
Data Visualizer

- Choose a ***Time Range***
  - Or look at the entire dataset
- Takes a sample of dataset
  - Select sample size from drop-down menu
  - Sample size is *per shard* ← discussed in Engineer I / II
- And returns some information about all fields in sample
  - Data type
  - Depending on data type:
    - distribution of values (numeric fields)
    - some statistics, like number of documents that have values
    - list of most frequent values

Elasticsearch Data Types for Fields

- **Simple Types, including**:
  - **text**: for full text (analyzed) strings
  - **keyword**: for exact value strings
  - **date** and **date_nanos**: string formatted as dates, or numeric dates
  - integer types: like **byte**, **short**, **integer**, **long**
  - floating-point numbers: **float**, **double**, **half_float**, **scaled_float**
  - **boolean**
  - **ip**: for IPv4 or IPv6 addresses
- **Hierarchical Types**: like **object** and **nested**
- **Specialized Types**: **geo_point**, **geo_shape**, **percolator, range** types and more

Demo



Instructor Demo

Lesson 1

Review - Data Visualizer

Summary

- Kibana Machine Learning has a Data Visualizer tool to get a quick overview of your data
- Elasticsearch stores documents using specialized data structures which you define by the field's data type
- Kibana's Discover Interface let's you further explore your data

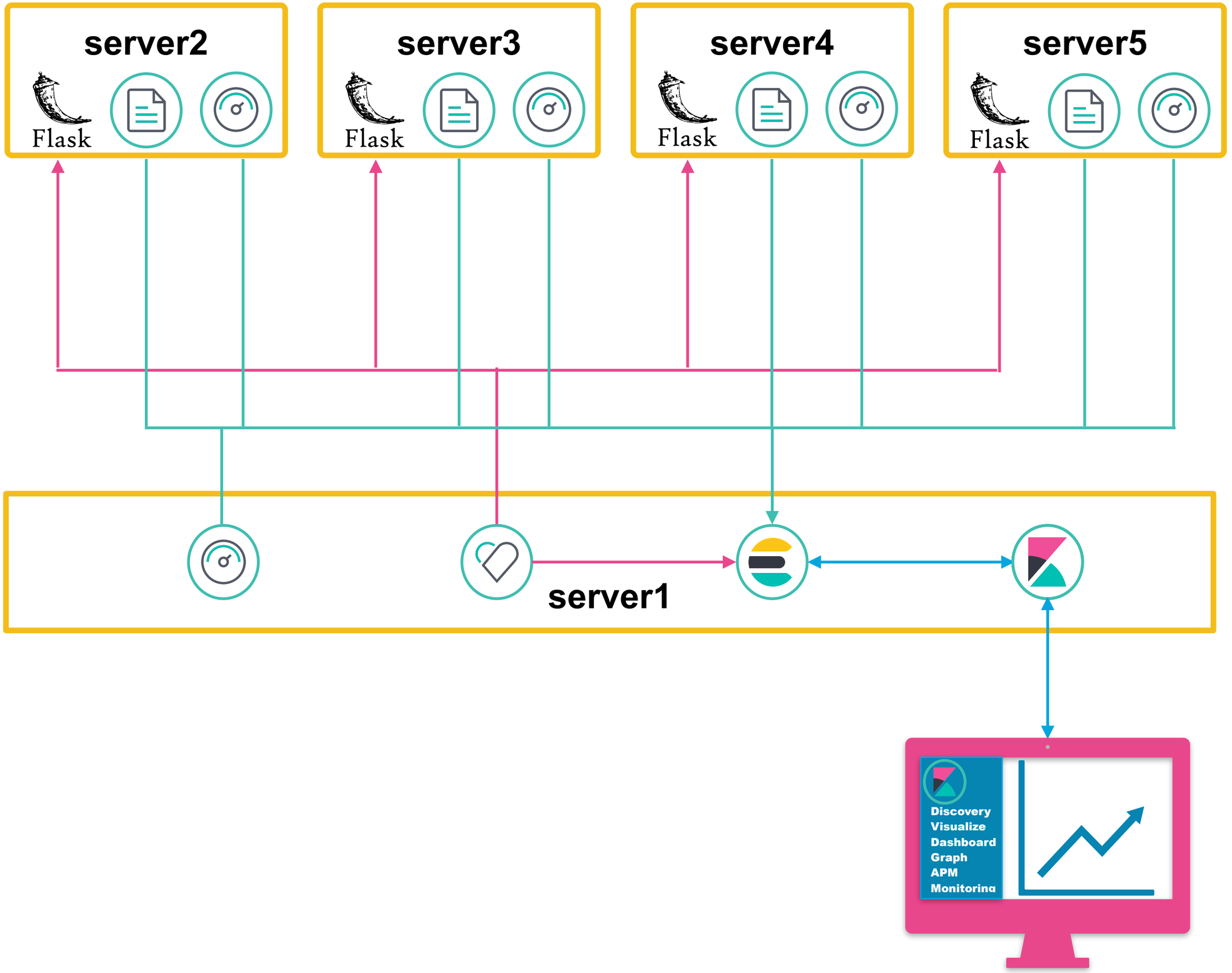
Quiz

1. **True or False**: Data is stored in Kibana.
2. **True or False**: Data Visualizer can only be used with Platinum subscription.
3. What is another tool you can use to explore your data?

Conclusions

Kibana Data and Ops Analyst

1. Kibana Fundamentals
2. Kibana Search
3. Kibana Visualizations
4. Kibana Dashboards
5. Kibana Visual Builder
6. Kibana Management
7. Observability Apps
8. Analyzing Infrastructure Data
9. Machine Learning and Alerting



Elastic Certification

- Hands-on, performance-based exams

Elasticsearch Engineer I

Elasticsearch Engineer II

Kibana Data and Ops Analyst

elastic

Thank You!

Please complete the online survey.

elastic

Quiz Answers

elastic

Introduction to Kibana

1. False. Kibana is stateless. All documents are stored in Elasticsearch.

2. False. Data Visualizer is available with the Basic license.

3. The Discover Interface enables you to explore your dataset by showing you some stats of a sampling of documents that match your search criteria.