Imagine your team is building a search feature for millions of records. How would you set up Elasticsearch, expose it via APIs, and make it easy for developers to query and use?

🔹 **Short Interview Answer**

- At a high level, Elasticsearch setup involves Install Elasticsearch (binary or Docker).
- Start a node → forms a cluster.
- Optionally add **Kibana** for visualization.
- Use **REST API (HTTP/JSON)** for interaction.
- Create indices, insert documents, search data.
- Store logs/app data as **JSON documents**.
- Visualize and monitor data in Kibana.

🔹 **Elasticsearch Setup**

1. **Install Elasticsearch**
   - Download from Elastic website or use package managers (apt, yum, brew).
   - Or run in **Docker** (most common for DevOps demos).
2. **Start Elasticsearch**
   - Runs as a service on port 9200 (default).
   - Example: http://localhost:9200
3. **Cluster & Node**
   - By default, you get **1 node cluster**.
   - In production, you configure **multiple nodes** for scalability & fault tolerance.
4. **(Optional) Add Kibana**
   - Install Kibana → connect to Elasticsearch.
   - Use browser dashboards for visualization.

🔹 **Elasticsearch API (High Level)**

- **REST API over HTTP** → You interact using JSON requests.
- Examples:
  1. **Check Cluster Health**

2. GET /_cluster/health
3. **Create an Index**
4. PUT /orders
5. **Insert a Document**
6. POST /orders/_doc
7. {
8. "order_id": "123",
9. "customer": "Abhijit",
10. "total": 250
11. }
12. **Search Documents**
13. GET /orders/_search
14. {
15. "query": { "match": { "customer": "Abhijit" } }
16. }

🔹 How to Use Elasticsearch in Practice

1. **Ingest Data**
   - Logs, metrics, or app data → sent via Logstash, Beats, or APIs.
2. **Store in Indices**
   - Data stored as JSON documents inside indices.
3. **Search & Analyze**
   - Developers/DevOps use APIs or Kibana queries to search logs, find errors, generate analytics.
4. **Visualize**
   - Kibana dashboards show real-time trends (errors, performance, usage).

Which is the **default port** Elasticsearch runs on?
A) 8080
B) 9200
C) 5601
D) 3306
Answer: B) 9200

Which of the following is NOT a common way to install Elasticsearch?
A) Using apt/yum/brew
B) Running via Docker
C) Compiling from scratch every time
D) Downloading from Elastic's website
Answer: C) Compiling from scratch every time

---

3. Cluster & Node
What happens if you start Elasticsearch without extra configuration?
A) It creates a 3-node cluster by default
B) It creates a single-node cluster

C) It won’t start until Kibana is installed
D) It only runs in read-only mode
Answer: B) It creates a single-node cluster

Why do we typically add **Kibana** to Elasticsearch setup?
A) To manage cluster nodes
B) To visualize and analyze data with dashboards
C) To replace Elasticsearch REST API
D) To handle log ingestion
Answer: B) To visualize and analyze data with dashboards

How do you interact with Elasticsearch?
A) Using SQL queries directly
B) REST API over HTTP with JSON
C) Only via Kibana GUI
D) Through a special desktop app
Answer: B) REST API over HTTP with JSON
