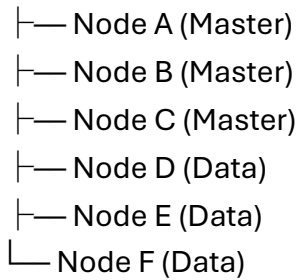


Structure of ELK

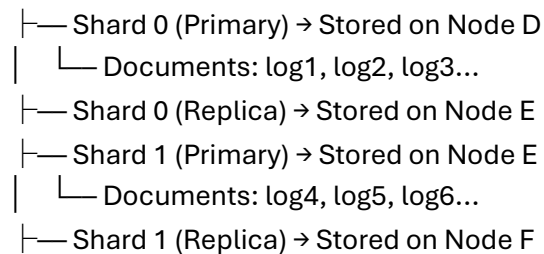
1. Elasticsearch Hierarchy – Simple Structure

Cluster



2. Index – Like a Database Table

Index: logs-2025-06



- ◆ Index = A collection of documents (like a table in SQL)
- ◆ Shards = Pieces of the index for horizontal scaling
- ◆ Primary shard = Main copy
- ◆ Replica shard = Backup copy for redundancy

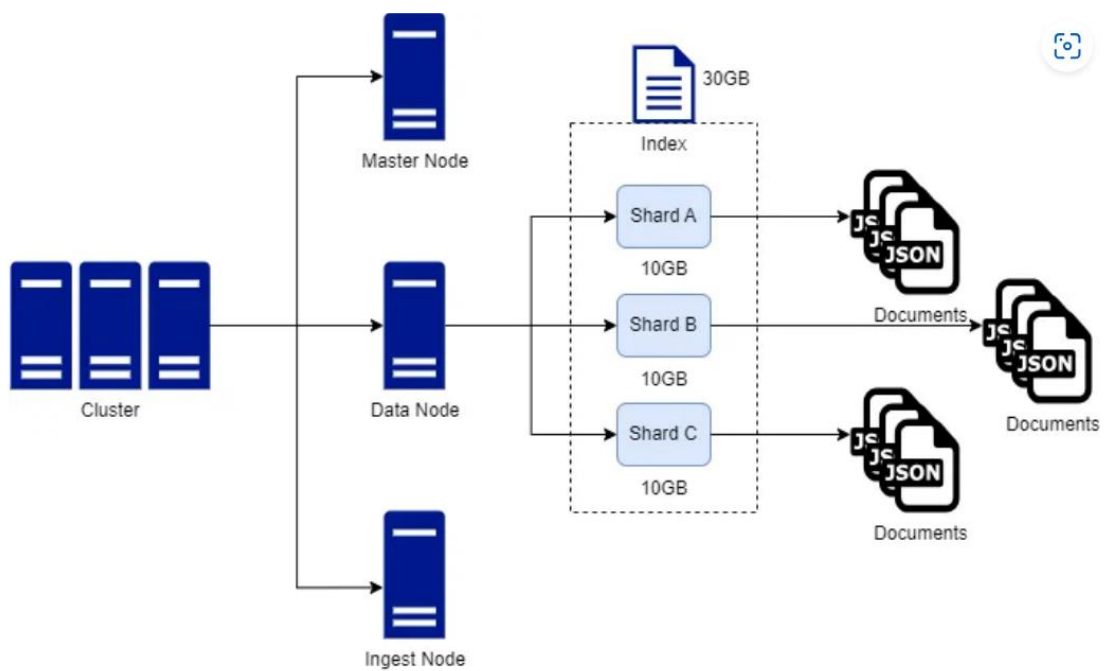
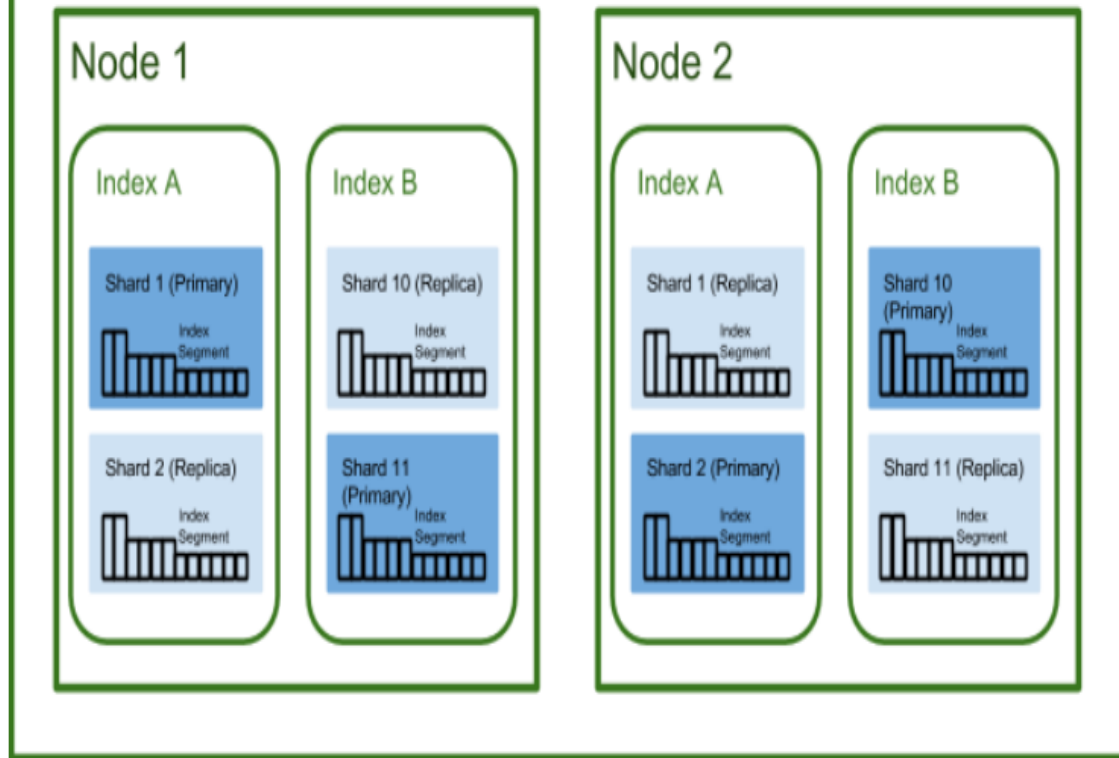
3. Document – Like a Row in SQL

Each document is a JSON object:

```
{
  "timestamp": "2025-06-13T12:34:56",
  "level": "ERROR",
  "message": "Failed to connect to DB"
}
```

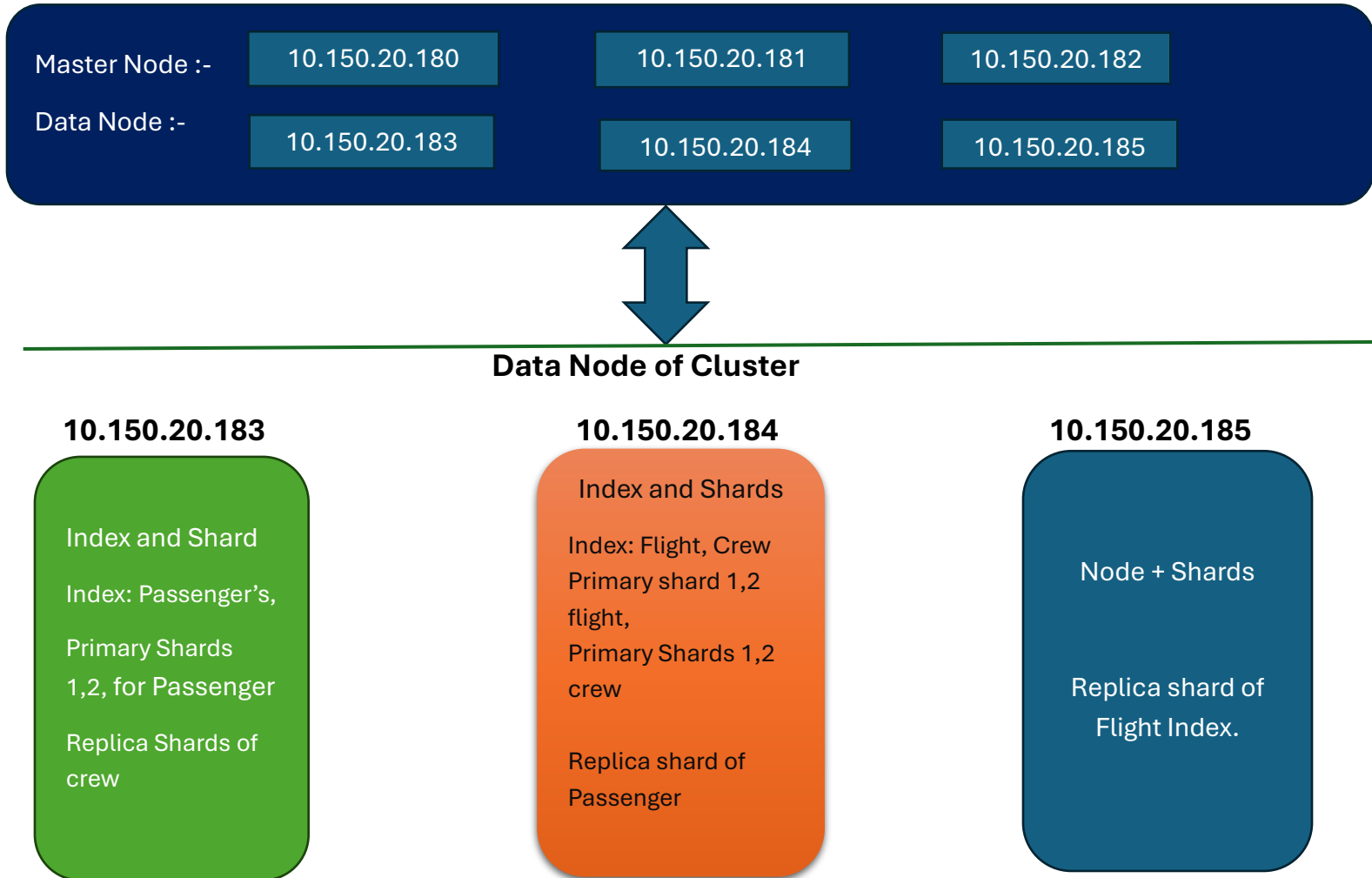
Documents are stored inside shards, which are stored inside data nodes.

ElasticSearch Cluster



Elastic design in DGARM

Cluster name:- elastic-nonprod



Master Node :- 10.150.20.180, 10.150.20.181, 10.150.20.182

Managing cluster state

Creating or deleting indices

Tracking which nodes are part of the cluster

Allocating shards to nodes

Monitoring node health and initiating recovery if needed

- ⇒ 1. Node 10.150.20.180 (Active Master)
- One of the nodes (likely A) is elected as the active master. It handles all cluster coordination tasks.
 - The election is based on a quorum (majority) of master-eligible nodes.

⇒ 2. Node 10.150.20.181 and 10.150.20.182 (Standby Masters)

These nodes are master-eligible but not currently active.

They monitor the active master and are ready to take over if Node A fails.

This ensures high availability and fault tolerance.