**ELK ILM Policy and Index Rotation**

**Introduction to Index Lifecycle Management (ILM)**

Index Lifecycle Management (ILM) is a feature in Elasticsearch that helps manage indices efficiently throughout their lifecycle. It automates tasks like rollover, shrinking, and deletion to optimize performance and storage costs.

**Key Phases of ILM Policy**

An ILM policy consists of the following phases:

1. **Hot Phase**: Active data ingestion and search.
2. **Warm Phase**: Optimized for read-only queries, force merging for better performance.
3. **Cold Phase**: Less frequent access, stored on lower-cost hardware.
4. **Forzen**:
5. **Delete Phase**: Data is no longer needed and gets deleted.

**Steps to Create an ILM Policy**

1. Define the policy with different phases.
2. Attach the policy to an index template.
3. Verify ILM policy execution.

**Example ILM Policy**

{

"policy": {

"phases": {

"hot": {

"actions": {

"rollover": {

"max\_size": "50gb",

"max\_age": "30d"

}

}

},

"warm": {

"actions": {

"readonly": {},

"forcemerge": {

"max\_num\_segments": 1

}

}

},

"delete": {

"min\_age": "90d",

"actions": {

"delete": {}

}

}

}

}

}

**Index Rotation**

Index rotation is the process of creating new indices based on conditions like time, size, or document count. It ensures better query performance and efficient storage management.

**Methods for Index Rotation**

1. **Time-based Rotation**: Create new indices daily, weekly, or monthly.
2. **Size-based Rotation**: Create new indices when the index reaches a specific size.
3. **Document Count-based Rotation**: Create new indices when a certain number of documents are indexed.

**Configuring Index Templates for ILM**

1. Create an index template and associate it with an ILM policy.
2. Ensure aliases are set up for seamless data ingestion.

**Example Index Template**

{

"index\_patterns": ["logs-\*"],

"settings": {

"index.lifecycle.name": "my-ilm-policy",

"index.lifecycle.rollover\_alias": "logs"

}

}

**Verifying ILM Execution**

* Check ILM policy execution: GET \_ilm/policy
* Monitor ILM status of an index: GET logs-\*/\_ilm/explain
* Force ILM execution if needed: POST logs-000001/\_ilm/move?phase=warm

**Conclusion**

ILM and Index Rotation help in managing indices efficiently, reducing storage costs, and improving performance. Teaching students how to implement ILM policies ensures they can maintain ELK clusters effectively.