Configure Log Retention Policy

Since **Elasticsearch** stores logs in indices, we can set up a 2-day retention policy using an Index Lifecycle Policy (ILM).

Create a policy:

```
curl -X PUT "http://elasticsearch:9200/_ilm/policy/2-day-retention" -H "Content-Type:
application/json" -d '{
 "policy": {
  "phases": {
   "hot": {
    "actions": {
     "rollover": {
      "max_age": "1d"
     }
    }
   },
   "delete": {
    "min_age": "2d",
    "actions": {
     "delete": {}
    }
   }
  }
 }
}'
```

Apply it to the index pattern:

```
curl -X PUT "http://elasticsearch:9200/kubernetes-logs-*/_settings" -H "Content-Type:
application/json" -d '{
 "index.lifecycle.name": "2-day-retention"
}'
```

Create a Kibana Dashboard for Log Analysis

Described in Task –1

Setup Metrics Visualization & Alerts

Described in Task –1

Setup Alerting in Kibana

1. **Go to Kibana → Stack Management → Alerts & Rules**
2. **Create a Rule**
   a. Condition: If CPU usage > 80% for 5 minutes
   b. Action: Send an alert via **Slack, Email, or Webhook**