**ELK Master Class: Elasticsearch, Beats, Logstash, and Kibana**

### **Duration: 40 HRS**

### **Prerequisites:** Basic Linux Knowledge

### **Course Objective:**

Understanding the ELK Stack - Elasticsearch, Logstash, Kibana, and Beats. Learn installation, configuration, and practical use of each component for efficient data management, analysis, and visualization.

### **ELK Stack Version:** 8.x

### **Lab Requirement:** Koenig DC (CentOS 7)

## **Module 0 – Fundamentals**

### **1. Linux Basics**

* File system structure
* Basic commands (ls, cd, cp, mv, grep, sed, awk)
* User and permission management
* Process management
* Networking basics (ports, firewalls, netstat, curl)
* System monitoring (top, htop, iostat)

### **2. JSON Fundamentals**

* JSON syntax and structure
* Parsing and validation
* Working with JSON in Linux (jq command)
* JSON in Elasticsearch

### **3. YAML Basics**

* Difference between JSON and YAML
* YAML syntax and indentation rules
* Writing configuration files for ELK

### **4. Basic Networking & Security Concepts**

* HTTP/HTTPS basics
* RESTful APIs (CRUD operations)
* SSL/TLS encryption
* Role-Based Access Control (RBAC)

## **Module 1 - ELK Stack Course Overview**

* Introduction to Stack
* Stack Components
* Stack Architecture
* Use Cases
* Advantages and Disadvantages

## **Module 2 – Installation and Configuration**

* Pre-requisites
* **Lab:** Elasticsearch Installation
* **Lab:** Kibana Installation
* **Lab:** Verify Installation

## **Module 3 - Elasticsearch**

* Introduction to Elasticsearch
* Elasticsearch Fundamentals
* Elasticsearch Architecture
* Elasticsearch REST APIs
* Types of APIs
* **Lab:** Document APIs
* **Lab:** Index APIs
* **Lab:** Search APIs
* **Lab:** Cluster APIs
* **Lab:** Aggregation APIs
* **Lab:** Query DSL
* **Lab:** Elasticsearch Queries

## **Module 4 - Kibana**

* Introduction to Kibana
* Kibana Fundamentals
* Kibana Search
* **Lab:** Kibana Visualizations
* **Lab:** Kibana Dashboards
* **Lab:** Kibana Management (Index Lifecycle Management, Alerting Using Watcher)

## **Module 5 - Logstash**

* Introduction to Logstash
* **Lab:** Installing Logstash
* **Lab:** Setup Logstash Pipeline for Ingesting Data into Elasticsearch
* Logstash Plugins
  + Input Plugins
  + Output Plugins
  + Filter Plugins
* Grok
* Queue Management in Logstash

## **Module 6 - Beats**

* Introduction to Beats
* Beats Use-cases
* **Lab:** File beat Installation and Configuration
* **Lab:** File beat for Shipping Logs from Client to Elastic Cluster

## **Module 7 - Logging & Monitoring**

* Introduction to Logging & Monitoring
* Fluentd and FluentBit
* Grok
* Sharding
* APM in Elasticsearch
* Replicas in Elasticsearch
* EFK (Elasticsearch, Fluentd/FluentBit, Kibana) with Grafana for Visualization