ELK Master Class - Elasticsearch, Beats, Logstash and Kibana

Duration: 32 Hours (4 Days)

Overview

The "ELK Master Class - Elasticsearch, Beats, Logstash, and Kibana" course is an in-depth training program designed to provide learners with comprehensive knowledge and hands-on experience in the ELK stack, which combines Elasticsearch, Logstash, and Kibana (ELK). This course covers all the essential elements, from the foundational understanding of the stack's architecture and components to the practical aspects of installation, configuration, and management.By delving into each part of the stack, participants will learn about Elasticsearch's powerful Search and data indexing capabilities, Kibana's data visualization tools, Logstash's data processing pipelines, and how Beats simplifies data collection. The course is structured to build expertise in managing and monitoring the ELK stack, Deploying real-world use cases, and overcoming common challenges. With this knowledge, learners can effectively implement and maintain an ELK stack for processing and visualizing large datasets in various environments.

Audience Profile

The ELK Master Class at Koenig Solutions is designed for professionals seeking expertise in Elasticsearch, Beats, Logstash, and Kibana for data analysis and visualization.

- Data Engineers
- DevOps Engineers
- System Administrators
- IT Operations Staff
- Search and Analytics Engineers
- Security and Incident Response Analysts
- Software Developers
- Data Scientists
- Business Intelligence (BI) Professionals
- Technical Architects
- Cloud Infrastructure Engineers
- Monitoring and Observability Personnel

Course Syllabus

Prerequisites: Basic Linux Knowledge

Course Objec1ve: Understanding the ELK Stack - Elas5csearch, Logstash, Kibana, and Beats.

Learn installa5on, configura5on, and prac5cal use of each component for efficient data

management, analysis, and visualiza5on

ELK Stack Version: 8.x

Lab Requirement: Koenig DC (CentOS 7)

Module 1 - ELK Stack

- Course Overview
- Introduc;on to Stack
- Stack Components
- Stack Architecture
- Use Cases
- Advantages and Disadvantages

Module 2 – Installa1on and Configura1on

- Pre-requisites
- Lab: Elas;csearch Installa;on
- Lab: Kibana Installa;on
- Lab: Verify Installa;on

Module 3 - Elas1csearch

- Introduc;on to Elas;csearch
- Elas;csearch Fundamentals
- Elas;csearch Architecture
- Elas;csearch REST APIs
- Types of APIs
- Lab: Document APIs
- Lab: Index APIs
- Lab: Search APIs
- Lab: Cluster APIs
- Lab: Aggrega;on APIs
- Lab: Query DSL
- Lab: Elas;csearch Queries

Module 4 - Kibana

- Introduc;on to Kibana
- Kibana Fundamentals
- Kibana Search
- Lab: Kibana Visualiza;ons
- Lab: Kibana Dashboards
- Lab: Kibana Management like Index Lifecycle Management
- Aler;ng Using Watcher

Module 5 - Logstash

- Introduc;on to Logstash
- Logstash Plugins
- Input Plugins
- Output Plugins
- Filter Plugins
- Lab: Installing Logstash
- Lab: Setup Logstash Pipeline for Inges;on of Data into Elas;csearch
- Queue Management at Logstash

Module 6 - Beats

- Introduc;on to Beats
- Beats Use-cases
- Lab: Filebeat Installa;on and Configura;on
- Lab: Filebeat for Shipping Logs from Client to Elas;c Cluster