ELK Master Class

Elasticsearch, Beats, Logstash and Kibana

Duration: 4 Days (8hrs/day)

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 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 like Index Lifecycle Management

Alerting Using Watcher

Module 5 - Logstash

Introduction to Logstash

Logstash Plugins

Input Plugins

Output Plugins

Filter Plugins

Lab: Installing Logstash

Lab: Setup Logstash Pipeline for Ingestion of Data into Elasticsearch

Queue Management at Logstash

Module 6 - Beats

Introduction to Beats

Beats Use-cases

Lab: Filebeat Installation and Configuration

Lab: Filebeat for Shipping Logs from Client to Elastic Cluster