"Mastering Elasticsearch 9.x: Data Management to Security Operations"

Duration: 8 Days (8 hours/day)
Version: Elasticsearch 9.x
Lab Requirement: 3-node Cluster using Docker (CentOS | Windows)
Prerequisites: Basic Linux Knowledge and Elasticsearch Administration Knowledge

Course Introduction:

Welcome to the comprehensive training program on Elasticsearch 9.x, designed to equip you with in-depth knowledge and practical skills for managing, ingesting, and analyzing data. This course will guide you through the essential components and advanced features of Elasticsearch, focusing on observability and security use cases across diverse industries. By the end of this program, you will be adept at deploying robust Elasticsearch solutions tailored to your organization's needs.

Module 1: Introduction to Elasticsearch 9.x

• Training Objectives and Environment Context: Understand the key learning goals and the setup required for a successful training experience.

• Elasticsearch 9.x Overview: Gain foundational knowledge of Elasticsearch's architecture and its role in modern data ecosystems.

• Observability and Security Use Cases: Explore how Elasticsearch can be applied to monitor systems and secure data infrastructures.

Module 2: Data Management

• Data Streams Architecture and Design: Learn about the structure and design principles of data streams in Elasticsearch.

• Index Lifecycle Management (ILM): Understand ILM policies to automate index management and optimize performance.

• Retention Strategies: Explore techniques for retaining data efficiently while balancing storage costs.

• Data Tiering and Storage Optimization: Learn methods for categorizing data based on usage patterns and optimizing storage.

Module 3: Data Ingestion

• Kafka + Logstash Integration: Delve into building flexible ingestion pipelines using Kafka and Logstash.

• Ingestion Architecture Best Practices: Identify best practices for designing robust and scalable ingestion architectures.

• Pipeline Design and Optimization: Optimize data pipelines for performance and reliability.

• OpenTelemetry Integration: Integrate OpenTelemetry for comprehensive telemetry data collection.

• OTel/EDOT Collectors: Understand the configuration and deployment of OpenTelemetry collectors.

• Ingesting Logs, Metrics, and Traces: Learn to handle diverse telemetry data types within Elasticsearch.

• End-to-End Telemetry Pipeline: Construct a seamless pipeline from data collection to analysis.

Module 4: Observability

• Application Performance Monitoring (APM): Monitor backend applications to identify performance bottlenecks.

• Backend Application Monitoring: Implement monitoring solutions for backend systems.

• Real User Monitoring (RUM): Capture real user interactions to enhance frontend performance.

• Frontend-to-Backend Performance Visibility: Achieve holistic visibility from user interaction to backend processing.

Module 5: Search, Querying, and Analytics

• Querying Fundamentals: Master the core concepts of searching and querying within Elasticsearch.

• Search APIs: Learn to leverage Elasticsearch's powerful search APIs for complex queries.

• Aggregations: Explore aggregation frameworks to summarize and analyze large datasets.

• Troubleshooting Workflows: Develop workflows to identify and resolve issues efficiently.

• Investigation and Root Cause Analysis: Conduct in-depth analyses to uncover underlying problems.

Module 6: AI and Machine Learning

• Predictive Analytics: Utilize machine learning models to predict future trends and behaviors.

• Anomaly Detection: Detect anomalies in data streams to preemptively address potential issues.

• Observability and Security Use Cases: Implement AI-driven solutions for enhancing observability and security.

Module 7: Security Operations and Automation

• SOAR Concepts: Understand Security Orchestration, Automation, and Response frameworks.

• Native Elastic Workflows: Leverage Elasticsearch's native capabilities for security operations.

• Playbooks and Automated Response: Design and implement automated response playbooks for efficient security management.

Module 8: Cluster Performance and Scaling

• Shard Strategy: Develop strategies for shard allocation and management to optimize performance.

• Monitoring and Troubleshooting: Implement monitoring solutions to detect and resolve cluster issues.

• Scaling for Growing Data Volumes: Plan and execute scaling strategies to accommodate increasing data loads.

Module 9: Elastic 9.x Best Practices

• Architecture Design: Design Elasticsearch architectures that align with best practices for performance and reliability.

• Operational Governance: Establish governance frameworks to ensure sustainable operations.

• Version-Specific Recommendations: Stay informed on the latest version-specific enhancements and recommendations.