XLSKILL PROFESSIONAL TRAINING

Excel Your Skill

Learn | Apply | Perform

ELK STACK COURSE OUTLINE

A structured, industry-focused training roadmap covering ELK administration, observability, monitoring, security, automation, and cloud deployment for real-world implementation.

Practical assignments, guided labs, demonstrations, and hands-on practice are integrated throughout the course to build real-world ELK implementation skills.

XLSKILL

- Windows + Linux + Cloud
- Hands-On
- 33 Modules
- Updated with additional advanced modules
- Labs, Assignments & Use Cases
- Structured Learning Path
- AWS, Elastic Cloud & Deployment
- Certificate
- Career Ready
- Elastic Certified Observability Engineer Exam
- Resume, Profile & Q&A Support

Address: Xion Mall, 2nd Floor, Office No. 202, Near Hinjewadi D-Mart, Hinjewadi Wakad Road, Hinjewadi, Pune 411057

Phone: 9850965096 | **Email:** info@xlskill.com | **Website:** www.xlskill.com

Enquiry & Admission Support

Ready to join the ELK Stack program? Contact XLSkill for batch details, enrollment guidance, and personalized course assistance.

VISIT US Address: Xion Mall, 2nd Floor, Office No. 202, Near Hinjewadi D-Mart, Hinjewadi Wakad Road, Hinjewadi, Pune 411057	**CALL / WHATSAPP** Phone: 9850965096
EMAIL US Email: info@xlskill.com	**VISIT WEBSITE** Website: www.xlskill.com

Course Overview

This is a comprehensive, practical ELK Stack course designed to take you from foundational concepts to advanced deployment. The curriculum thoroughly covers Elasticsearch, Logstash, Kibana, Beats, observability, security, monitoring, cloud deployment, and system architecture. Students will gain the skills necessary to build robust log analytics and observability pipelines.

Learning Outcomes

- Understand and deploy the complete ELK Stack architecture.
- Collect, parse, and transform complex data using Logstash and Beats.
- Secure Elasticsearch clusters using Role-Based Access Control (RBAC) and Field-Level Security.
- Monitor applications and infrastructure using Heartbeat, Metricbeat, and APM.
- Create interactive, real-time dashboards and visualizations in Kibana.
- Manage index lifecycles (ILM) and execute snapshot/restore operations for data safety.
- Set up automated alerts and notifications using Watcher and Kibana Rules.
- Deploy and manage the ELK Stack across Windows, Linux, AWS, and Elastic Cloud environments.

Who Should Attend

- IT Students and Graduates
- System Administrators
- DevOps Engineers
- Support and Operations Engineers
- Security Operations Center (SOC) Analysts

- Anyone interested in log analytics, observability, and data visualization

Course Structure

This training combines in-depth theoretical explanation, live demonstrations, guided labs, and independent assignments to reinforce learning objectives.

Address: Xion Mall, 2nd Floor, Office No. 202, Near Hinjewadi D-Mart, Hinjewadi Wakad Road, Hinjewadi, Pune 411057

Phone: 9850965096 | **Email:** info@xlskill.com | **Website:** www.xlskill.com

Detailed Modules

1. Introduction to ELK Stack

- What is Elasticsearch?
- Current data analysis problems in the industry
- Overview of ELK Stack components (Elasticsearch, Logstash, Kibana, Beats)
- Understanding how ELK works together
- Real-world use cases of the ELK Stack
- Installation methods and deployment strategies

2. Introduction to Elasticsearch

- Core concepts of Elasticsearch
- Installing and setting up Elasticsearch on Windows
- Q&A Session

3. Introduction to Kibana

- What is Kibana?
- Installing and setting up Kibana on Windows
- High-level overview of the Kibana UI
- Q&A Session
- Hands-on Assignment Included

4. Introduction to Heartbeat

- What is Heartbeat?
- Why Heartbeat is needed for uptime monitoring
- Installing and setting up Heartbeat on Windows
- Q&A Session

5. Introduction to Synthetic Monitoring

- What is synthetic monitoring?
- Differences between Heartbeat and synthetic monitoring
- Understanding SLA (Service Level Agreement) and SLO (Service Level Objective)
- SLA and SLO configuration
- Q&A Session

6. Metricbeat and Stack Monitoring

- Introduction to Metricbeat
- Different modules available in Metricbeat
- What is stack monitoring?
- Configuring stack monitoring using Kibana

7. Winlogbeat

- Introduction to Winlogbeat and its primary use cases

8. Introduction to Filebeat

- What is Filebeat and why use it?
- Setting up Filebeat to collect system logs

- Configuring Winlogbeat in Windows environments

- Reading multiple paths/files using Filebeat
- Understanding processors in Filebeat
- Multiline pattern basics
- Basic modules in Filebeat (Elasticsearch, Kibana, System)
- Q&A Session
- Hands-on Assignment Included

Address: Xion Mall, 2nd Floor, Office No. 202, Near Hinjewadi D-Mart, Hinjewadi Wakad Road, Hinjewadi, Pune 411057

Phone: 9850965096 | **Email:** info@xlskill.com | **Website:** www.xlskill.com

9. Introduction to Logstash

- What is Logstash and why is it essential?
- Setting up Logstash on Windows
- Logstash pipeline architecture (Input, Filter, Output)
- Common Logstash input plugins
- Common Logstash filter plugins (Grok, Mutate, Date, JSON, XML, CSV, etc.)
- Common Logstash output plugins
- Creating a single Logstash pipeline
- Working with multiple Logstash pipelines
- Centralized Logstash pipeline management using Kibana
- Calling one Logstash pipeline from another
- Pipeline workers, batch size, and batch delay concepts
- Dead letter queues and persistent queues
- Performance tuning for Logstash servers
- Q&A Session
- Hands-on Assignment Included

10. Ingest Pipelines

- What is an ingest pipeline?
- Differences between Logstash and ingest pipelines
- Using processors to transform data efficiently
- Hands-on: Creating an ingest pipeline
- When to use ingest pipelines vs. Logstash
- Hands-on Assignment Included

11. Basic Terminology & Architecture

- Understanding clusters, nodes, indices, and documents
- Shards, replicas, primary shards, and replica shards
- Detailed look at how documents are processed into Elasticsearch

12. Making Your Data Secure

- What is RBAC and why is security critical?
- User authentication and authorization in Kibana
- Enabling authentication and Role-Based Access Control (RBAC)
- Implementing field-level security
- Kibana Spaces and their practical usage
- Hands-on security practice
- Hands-on Assignment Included

13. Index Lifecycle Management

14. Index Templates, Mapping,

(ILM)

- What is ILM and why use it?
- Different data tier zones available
- Automating index rollover and retention policies
- Hands-on: Configuring an ILM policy

and Component Templates

- Index templates and mappings (static vs. dynamic) in Elasticsearch
- Component templates and their usage
- Hands-on: Creating custom mappings
- Hands-on Assignment Included

Address: Xion Mall, 2nd Floor, Office No. 202, Near Hinjewadi D-Mart, Hinjewadi Wakad Road, Hinjewadi, Pune 411057

Phone: 9850965096 | **Email:** info@xlskill.com | **Website:** www.xlskill.com

15. Snapshot and Restore

- What are snapshot and restore operations?
- Hands-on: Creating snapshots for local storage
- Managing policies and data restoration workflows
- Hands-on Assignment Included

16. Data Discovery and Visualization in Kibana

- Using the Discover interface to explore raw data
- Creating custom dashboards and advanced visualizations
- Hands-on Assignment Included

17. Licensing, Version History, and Compatibility

- Understanding the Elastic licensing model
- Versioning best practices and navigating the compatibility matrix

18. Alerting with Watcher

- What is an alert connector?
- Introduction to Watcher in the ELK ecosystem
- Creating connectors for Email, Zoom, Indices, and Microsoft Teams
- Creating threshold-based alerts and advanced Watcher scripts
- Configuring Watcher for email and webhook-based alerts
- Sharing reports and dashboards via Watcher
- Hands-on Assignment Included

19. Rule Creation

- What are Kibana rules?
- Differences between Kibana rules and Watcher
- Creating custom monitoring rules
- Stack monitoring alert rules
- Hands-on Assignment Included

20. SIEM (Security Information and Event Management)

- Introduction to SIEM concepts
- Implementing SIEM with the ELK Stack
- Hands-on: Setting up a practical SIEM use case
- Hands-on Assignment Included

21. Basic DSL Querying

- Introduction to Query DSL
- Understanding the differences between DSL, KQL, EQL, and ES|QL
- Day-to-day useful queries for administrators and analysts
- Hands-on: Writing custom DSL queries

22. Introduction to APM (Application Performance Monitoring)

- APM concepts and architecture
- Configuring the APM Server
- Instrumenting applications with the APM Agent
- Integrating APM with Elasticsearch

Address: Xion Mall, 2nd Floor, Office No. 202, Near Hinjewadi D-Mart, Hinjewadi Wakad Road, Hinjewadi, Pune 411057

Phone: 9850965096 | **Email:** info@xlskill.com | **Website:** www.xlskill.com

23. Machine Learning and Anomaly Detection

- Introduction to Machine Learning capabilities in ELK
- Configuring detection rules and data forecasting

24. Elastic Agent and Fleet Management

- Introduction to Fleet management in ELK
- Configuring Fleet agents and Elastic Agents
- Creating and managing deployment policies
- Navigating the Fleet UI and system settings
- Understanding the difference between indices and data streams
- Hands-on Assignment Included

Additional Linux & AWS Coverage

The following modules expand your skills by bringing the ELK stack into enterprise-grade Linux and Cloud environments.

25. Basic Introduction to Linux and AWS

- Core concepts of Linux system administration and Amazon Web Services
- Creating an AWS account
- Launching and configuring Virtual Machines (EC2)

26. Cluster Sizing and Architecture

- How to architect a production-ready cluster
- Best practices for performance and high availability
- Key design questions to ask before deployment

27. Cluster Creation with RPM and TAR

- Creating a 2-node secure Elasticsearch cluster using RPM packages
- Understanding and implementing CA, SSL, HTTP, and TLS certificates
- Securely connecting other components to the Elasticsearch cluster
- Creating a 2-node Elasticsearch cluster using TAR archives

28. Cross-Cluster Concepts

- What is cross-cluster search (CCS) and cross-cluster replication (CCR)?
- Configuring and managing cross-cluster features

- Launching and securing Kibana in a Linux environment

Address: Xion Mall, 2nd Floor, Office No. 202, Near Hinjewadi D-Mart, Hinjewadi Wakad Road, Hinjewadi, Pune 411057

Phone: 9850965096 | **Email:** info@xlskill.com | **Website:** www.xlskill.com

29. Upgrading the Cluster

- Best practices and pre-flight checks for ELK version upgrades
- Safely upgrading a 2-node Elasticsearch cluster
- Upgrading Kibana, Logstash, and Beats agents

30. Snapshot and Restore with AWS S3

- Configuring and attaching an AWS S3 bucket as a snapshot repository

31. Logstash Configuration with S3

- Configuring Logstash pipelines to read data directly from an S3 bucket

32. Elastic Cloud Deployment and Management

- Deploying the ELK Stack rapidly on Elastic Cloud
- Enabling and managing deployment audit logs
- Performing stack upgrades within Elastic Cloud
- Deploying configuration changes safely
- Best practices for handling support cases with Elastic

Advanced modules added as per updated outline

33. Elasticsearch Troubleshooting & Cluster Health Analysis

- Cluster Health Analysis (Red, Yellow, Green)
- Unassigned Shards and Shard Allocation Explain API
- Cluster Recovery and Master Election Issues
- Disk Watermark and Read-Only Index Problems
- High Heap, High CPU and GC Troubleshooting
- Slow Queries, Search Profiling and Thread Pool Rejections
- Circuit Breaker Exceptions and Diagnostic Collection

34. Elasticsearch Performance Tuning

- Query Optimization Techniques
- Mapping and Index Design Best Practices
- Shard Sizing Strategy
- Bulk Indexing Optimization
- Refresh Interval and Force Merge Tuning
- Cache Management and Search Performance
- Hot-Warm-Cold-Frozen Architecture Design

Address: Xion Mall, 2nd Floor, Office No. 202, Near Hinjewadi D-Mart, Hinjewadi Wakad Road, Hinjewadi, Pune 411057

Phone: 9850965096 | **Email:** info@xlskill.com | **Website:** www.xlskill.com

35. Elastic Agent & Fleet Migration Project

- Beats to Elastic Agent Migration Strategy
- Fleet Architecture and Deployment Models
- Agent Policies and Integrations
- Data Streams vs Traditional Indices
- Production Migration Planning and Rollback Strategy

36. Real Enterprise Use Cases

- Infrastructure Monitoring Use Case
- Application Monitoring Use Case
- SIEM Implementation Example
- Windows and Linux Monitoring
- API and Cloud Monitoring
- End-to-End Observability Project

37. Elasticsearch APIs & Administration

- CAT APIs
- Cluster APIs
- Node APIs
- Index APIs
- Security APIs
- Snapshot and Recovery APIs

38. Real Production Architecture & Client Projects

- Multi-node Production Cluster Design
- Hot/Warm/Cold Architecture
- Elastic Cloud Architecture
- Cross Region DR Design
- Sizing Calculations
- Real Customer Case Studies
- Support Ticket Handling
- Upgrade Planning
- Migration Planning

39. Career Support and Q&A

- Professional resume creation support
- Guidance on updating resumes, LinkedIn, and Naukri profiles for observability roles
- Open Questions and Answers session

XLSkill

Excel Your Skill — Learn | Apply | Perform

Professional IT Training for Analytics, Observability, and Modern Infrastructure Skills

P Mob / WhatsApp: 9850965096
E Email: info@xlskill.com
W Website: www.xlskill.com