

Elasticsearch in Action

Deploy, Search and Visualise

FA-0818 · 1 day

DevOps, Cloud & Infrastructure · Data & Analytics

Deploy Elasticsearch and Kibana on Ubuntu 24.04, index and query JSON data, and build a dashboard through a practical single-node workshop.

Introduction

Search becomes useful when teams can control how data is indexed, retrieve the right records, and turn results into information they can act on. Elasticsearch provides the search and analytics engine, while Kibana provides tools for exploring data and building visualisations. This course brings them together through practical, on-premises deployment on an Ubuntu 24.04 server.

Participants build a working single-node environment, load and query data, and create a usable Kibana dashboard. Deployment, security and troubleshooting are woven into the work so participants understand what happens beyond a successful installation. The focus is on practical decisions developers and DevOps practitioners make in their daily work.

Designed for experienced Linux, DevOps and programming practitioners, this one-day workshop follows a single-node training environment from deployment to a working dashboard. Production availability and backup are introduced as planning topics; a training deployment is not a highly available production cluster.

Learning outcomes

By the end of the course, participants will be able to:

- Deploy and connect Elasticsearch and Kibana on Ubuntu 24.04.
- Configure authenticated access, TLS and essential network restrictions.
- Create indices, define mappings and load JSON documents.
- Execute searches, filters and aggregations through REST APIs and scripts.
- Explore data and build visualisations and dashboards in Kibana.
- Check deployment health and explain backup and production-readiness requirements.

Prerequisites

- Good hands-on Linux administration experience, including package installation, permissions, systemd services and log inspection.
- Working DevOps experience deploying services and troubleshooting TCP/IP connectivity, firewall rules and TLS.
- Good hands-on programming experience, including writing scripts, handling JSON and calling REST APIs independently.
- A laptop or workstation with a current browser, terminal and SSH client.
- Access to an Ubuntu 24.04 training server with sudo privileges.
- Unrestricted internet access.
- Ability to establish SSH connections to remote training servers at public IP addresses, with outbound SSH permitted by the device and network.

Training outline

1. 1. Elasticsearch and Kibana Foundations

1. Search and analytics use cases
2. Nodes, clusters, indices, documents, shards and replicas
3. Kibana and the Elasticsearch REST APIs

2. 2. On-Premises Deployment on Ubuntu 24.04

1. Server preparation and resource planning
2. Version matching and APT package installation
3. Single-node configuration and systemd services
4. TLS, authentication and secure network access
5. Kibana enrolment and deployment verification

3. 3. Data Indexing and Modelling

1. Index creation and document operations
2. Mappings, field types, text and keyword fields
3. Text analysis fundamentals
4. Bulk ingestion of JSON documents

4. 4. Searching and Programmatic Access

1. Kibana Dev Tools Console and Query DSL
2. Full-text searches, Boolean queries and filters
3. Sorting, pagination and aggregations
4. Authenticated REST API calls from scripts

5. 5. Data Exploration and Dashboards in Kibana

1. Data views and Discover
2. KQL filtering and introductory ES|QL
3. Lens visualisations
4. Dashboard assembly and interactive filtering

6. 6. Essential Operations and Production Planning

1. Users, roles and restricted API keys
2. Cluster health, service logs and troubleshooting
3. Snapshot and restore fundamentals
4. Multi-node availability and production-readiness considerations

Disclaimer

This outline serves as a training guideline. The trainer reserves the right to amend the content, sequence or emphasis without prior notice to reflect participant needs, technical developments and delivery conditions, while remaining aligned with the course objectives.