

# AIOps for Kubernetes

Learn to apply AI and machine learning to Kubernetes operations, from observability and anomaly detection to predictive scaling and automated incident response.

**24 Hours**

DURATION

**6**

MODULES

**27**

TOPICS

**19**

HANDS-ON LABS

## COURSE OVERVIEW

This course covers the fundamentals of AIOps and the operational challenges of Kubernetes, starting with setting up a monitoring stack using Prometheus and Grafana. It then addresses integrating observability tools such as OpenTelemetry and the ELK stack with machine learning and large language models to label and summarize logs. Subsequent modules cover incident correlation and root cause analysis with graph models and LLMs, predictive scaling of workloads using Prophet and KEDA, and runtime security and threat detection with tools such as Falco and KubeArmor. The course concludes with building automated alert routing and AIOps workflows using LangChain and Ollama.

## WHO THIS COURSE IS FOR

**Kubernetes Administrators**

**Site Reliability Engineers**

**DevOps Engineers**

**Platform Engineers**

**Security Operations Engineers**

**Cloud Infrastructure Engineers**

## TOOLS AND REQUIREMENTS

Lab VM / Environment Requirements (Preferred/Ideal)

- OS: Ubuntu 22.04 LTS (native or WSL2)
- CPU: 8 cores (minimum for Ollama + K8s)
- RAM: 16 GB or more (essential for Ollama models + monitoring tools)
- Disk: 60 GB SSD or higher (Docker images, Ollama models, datasets)
- Tools: Docker, Minikube, Helm, kubectl, Ollama (installed via shell script)
- Python: 3.10+ with pip
- Editors: Jupyter Notebook or VSCode
- Python Libraries: pandas, numpy, matplotlib, scikit-learn, prophet, langchain, ollama
- Required: Neo4j Desktop (open-source)
- Ollama with the following models pulled: llama3.2:1b, llama3.2:3b, gemma3:1b, gemma3:3b
- Alerting Options: Local Mattermost, file-based logging, or email

# What You Will Learn

- Understand the fundamentals of AIOps and its necessity in modern Kubernetes environments
- Learn how to integrate monitoring, logging, and observability tools with ML models
- Apply AI/ML techniques for real-time anomaly detection, incident management, and root cause analysis
- Forecast resource usage and implement predictive scaling with AI models
- Implement open-source security tools with LLM-powered threat explanations
- Build smart workflows for alert routing and AIOps automation using LangChain and Ollama
- Deliver hands-on labs that simulate real-world operational challenges and AI-based solutions in Kubernetes

## COURSE SYLLABUS

## 6 Modules, 27 Topics

01

4 Labs

### Introduction to AIOps & Kubernetes

*Outcome: Understand AIOps concepts and set up a monitoring stack on Kubernetes.*

## THEORY

- AIOps fundamentals, reactive vs proactive vs predictive ops
- **Kubernetes complexity:** ephemeral workloads, scale, observability gaps

## TOOLS

- Prometheus, Grafana, Minikube, IsolationForest (Python), Prometheus, Grafana

## OUTPUTS

- Grafana dashboards showing CPU/memory usage patterns, sample anomaly metrics, Helm config files

02

3 Labs

### Monitoring & Observability with AI

*Outcome: Integrate observability tools and apply AI to label and summarize logs.*

## THEORY

- Metrics (Prometheus), Logs (ELK/Loki), Traces (OpenTelemetry)
- Observability pipelines in cloud-native environments

## TOOLS

- OpenTelemetry, ELK Stack, FluentBit, ML/LLM (LangChain)

## OUTPUTS

- Indexed logs, ML-labeled alerts, pipeline config files

**03****3 Labs**

## Incident Management & Root Cause Analysis

*Outcome: Use graph models and LLMs to explain incidents and derive root causes.*

### THEORY

- Incident correlation, noise reduction, NLP-based RCA using GPT
- Graph modeling with Neo4j

### TOOLS

- Neo4j, Ollama (local LLM), LangChain, Kubernetes logs

### OUTPUTS

- Root cause graph, GPT output summary, enriched logs

**04****3 Labs**

## Predictive Scaling & Optimization

*Outcome: Predict workload patterns and scale Kubernetes clusters automatically.*

### THEORY

- Limitations of HPA/VPA
- Event-driven scaling (KEDA)
- Forecasting with Prophet for predictive autoscaling

### TOOLS

- KEDA, Prophet, Python, HorizontalPodAutoscaler

### OUTPUTS

- Forecast plot, scaling configs, KEDA deployment

**05****4 Labs**

## Security, Threat Detection & Drift Enforcement

*Outcome: Detect and respond to runtime threats using behavioral analysis and LLMs.*

### THEORY

- Behavioral anomaly detection, drift detection
- **Tools:** Falco, Sysdig Secure, KubeArmor
- GPT for threat explanation

### TOOLS

- Falco, KubeArmor, Ollama, Python, shell scripts

### OUTPUTS

- Falco logs, LLM classification, remediation YAMLS

## AIOps Platforms & Smart Workflows

Outcome: Build end-to-end AIOps workflows for alert handling using open-source tools.

### THEORY

- DIY AIOps with LangChain + OpenAI
- Alert classification and routing
- **Market tools:** Dynatrace, Moogsoft, Splunk

### TOOLS

- LangChain, Ollama API, Slack Webhooks, Python

### OUTPUTS

- LangChain flow, alert messages, webhook config

## HANDS-ON LABS

# Practise What You Learn

| #  | MODULE                                                    | ACTIVITY                                                                                                                                                                                                                                                                                             |
|----|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 01 | <b>Introduction to AIOps &amp; Kubernetes</b>             | <ul style="list-style-type: none"> <li>■ Deploy Prometheus and Grafana using Helm charts</li> <li>■ Simulate CPU/memory usage using BusyBox or stress-ng</li> <li>■ Observe and visualize cluster metrics in Grafana</li> <li>■ Optionally export metrics for anomaly detection in Python</li> </ul> |
| 02 | <b>Monitoring &amp; Observability with AI</b>             | <ul style="list-style-type: none"> <li>■ Install OTEL Collector</li> <li>■ Ingest logs</li> <li>■ Label anomalies using ML or LLM</li> </ul>                                                                                                                                                         |
| 03 | <b>Incident Management &amp; Root Cause Analysis</b>      | <ul style="list-style-type: none"> <li>■ Load logs into Neo4j</li> <li>■ Use GPT to explain alerts</li> <li>■ Build cause-effect graph</li> </ul>                                                                                                                                                    |
| 04 | <b>Predictive Scaling &amp; Optimization</b>              | <ul style="list-style-type: none"> <li>■ Deploy KEDA</li> <li>■ Simulate variable load</li> <li>■ Forecast future usage and trigger autoscaling</li> </ul>                                                                                                                                           |
| 05 | <b>Security, Threat Detection &amp; Drift Enforcement</b> | <ul style="list-style-type: none"> <li>■ Deploy Falco</li> <li>■ Simulate attack</li> <li>■ Classify threat with GPT</li> <li>■ Auto-remediate (optional)</li> </ul>                                                                                                                                 |
| 06 | <b>AIOps Platforms &amp; Smart Workflows</b>              | <ul style="list-style-type: none"> <li>■ Create alert router using LangChain + GPT</li> <li>■ Send output to Slack</li> </ul>                                                                                                                                                                        |

#### WHAT IS INCLUDED

## Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

#### ABOUT KOENIG

## Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

#### FLEXIBLE DELIVERY

## Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

## Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit [koenig-solutions.com](https://koenig-solutions.com)

✉ [info@koenig-solutions.com](mailto:info@koenig-solutions.com)