ELASTIC OBSERVABILITY ENGINEER

Observability is achieved when you bring your logs, metrics, and APM traces together to create a complete picture of the health and activity of your infrastructure. This instructor-led course provides a strong foundation on using the Elastic Stack to implement unified observability with a single-stack solution. You will learn how to collect logs, metrics, and APM data, and then ship them to a single datastore — Elasticsearch. You will also learn how unified observability data can be made even more actionable through machine learning and alerting, as well as easier to correlate data across different sources. Using Kibana, you will also explore how to visualize your observability data through an intuitive user interface. After completing this course, you will be well on your way to becoming an Elastic Certified Observability Engineer.

LESSONS

All lessons include a hands-on lab.

Intro to observability

Observability is an aspect of a well-managed application or system. Learn how the pillars of observability — logs, metrics, and traces — work together within the Elastic Stack to provide insight into every aspect of a multi-layer application.Start with the most-common observability question: is the service alive? And then find the answer with Heartbeat and Uptime.

Metrics

The next observability question is: how healthy is the service? Memory, CPU, disk space, is our service running well? Learn how to configure Metricbeat to ship metric data to Elasticsearch, how modules can provide focused details about various servers and services, and how the Metrics app can show off the trouble spots quickly.

Continued on next page

COURSE INFORMATION

Audience
Software Developers
Software Engineers
Data Architects
System Administrators
DevOps

Duration
24 Hours

Language
English

Prerequisites
- No prior knowledge of the Elastic Stack required
- Working knowledge of Linux terminal commands and editors recommended

Requirements
- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (other browsers not supported)
- Disable any ad blockers and restart your browser before class

elastic

ELASTIC OBSERVABILITY ENGINEER

LESSONS

All lessons include a hands-on lab.

Logging

Observability level three: are there any errors or issues with the service? How many hits, how many errors, how does load change over time. Learn how to set up Filebeat to ship data to Elasticsearch using one-click, out-of-the-box integrations for most popular services. Then hop into the Logging app to tie your data together.

Structuring and processing data

If the logs don't fit a module, can they still be processed? Of course! Learn how to use Elasticsearch ingest nodes to collect data and handle and debug errors during ingest. Learn how to extract unstructured events using dissect patterns, and drop and remove entries that are not relevant. Also learn how to transform incoming data to conform to formats for dates and text, as well as load additional data from internal and external sources.

Application performance monitoring (APM)

The best way to find the source of errors and bottlenecks is to trace the code in and between the services. Learn how to use Elastic APM for monitoring software services and applications in real time. Learn about the different components of Elastic APM and how they work together to enable analysis of performance throughout the application architecture.

Analyzing observability data

Learn to use machine learning to provide detailed, ongoing analysis of observability data. Then learn to visualize your data in a variety of ways with preconfigured, editable dashboards. Finally, learn how to glue together all the sources for observability data using custom visualizations in Kibana.

Managing observability data

With so much data coming in, managing the data becomes a large task. Learn how to keep track of incoming data, how to manage the data lifecycle, and how to get the Elastic Stack to automatically handle these tasks.

Observing the observer

The final module teaches how alerting can be deployed to watch over the observability data and send alerts based on machine learning data (or any relevant SLA threshold). The observability cycle is completed by teaching how to stand up monitoring on the observability cluster itself to ensure the health of your Elastic Stack as it collects data.

elastic