STRUCTURING LOG DATA

LOGGING COURSE OUTLINE

Overview

Logs aren't always the easiest things to read, but Elasticsearch can help with that. This course teaches you how to structure your unstructured data using an Elasticsearch ingest node. Starting with a simple case of parsing a log file with a predefined parser, you will learn how to parse unstructured event data in hybrid cases using custom grok patterns. You will also learn how to handle and debug ingest errors along the way. After completing this course, you will be able to structure your log data however you want, regardless of its initial format.

Audience

Software Developers and Engineers, Data Architects, System Administrators, DevOps

Duration

2–3 hours

Language

English

Prerequisites

We recommend you have taken Elasticsearch Engineer I and Elasticsearch Engineer II or possess equivalent knowledge. Engineer I and Engineer II teach the concepts that are the foundation upon which all specializations are built.

Requirements

- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (Safari is not 100% supported)
- Due to virtual classroom JavaScript requirements, we recommend that you disable any ad-blockers and restart your browser before class.

LOGGING COURSE OUTLINE

STRUCTURING LOG DATA

Modules

Extracting Fields and Wrangling Data

- Learn why you need to structure unstructured data, as well as how to do it by extracting fields and wrangling data.
- **Hands-On Lab**

Combining Unstructured Text Patterns: Grok

- Learn how to use grok to combine text patterns to match any unstructured format. Also learn how to handle errors and debug them.
- **Hands-On Lab**

Advanced Grok

- Learn the details of a few hybrid cases and some best practices for handling them. See how to make custom grok patterns.
- **Hands-On Lab**

elastic