SHIPPING LOG DATA

LOGGING COURSE OUTLINE

Overview

Before you can analyze your logs, you need to get them into Elasticsearch. This course will teach you how to set up and ship data with Filebeat, a light-weight data shipper that can tail multiple files at once and ship the data to your Elasticsearch cluster. In addition to shipping file data like logs, Filebeat can also tag data, parse multi-line log entries, and use conditionals to make decisions about what to do with each log line. This class covers these topics and more, including building resiliency and monitoring Filebeat. After completing this course, you will be able to easily tail and ship your logs to Elasticsearch with Filebeat.

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

SHIPPING LOG DATA

Modules

Filebeat Introduction, Architecture, and Outputs

- Learn how Filebeat can be used for your logging needs and how to ship data to Elasticsearch from different sources. Also learn what prospectors, harvesters, and spoolers are and how they're used.

- **Hands-On Lab**

Modules & Outputs

- Explore the different Filebeat modules and see how to use them. Also learn about tagging, pipelines, and conditionals.

- **Hands-On Lab**

Resilience

- Learn how to handle new files, recover and roll over existing files, and how to monitor Filebeat.

- **Hands-On Lab**

Multi-Line Processing

- Explore the concept of handling files with multiple lines.

- **Hands-on Lab**

elastic