Logging with OpenTelemetry

This is a hands-on, developer-centric workshop showcasing various methods for working with OpenTelemetry logs and Elastic.

Background

The advent of OpenTelemetry has forever changed how we capture observability signals. While OTel initially focused on delivering traces and metrics, support for collection of logs is now stable and gaining adoption, particularly in Kubernetes environments.

In this lab, we will explore several state-of-the-art models for using OpenTelemetry to collect and parse logs. Participants will be “hands-on-keyboard”, modifying code and OTel configurations.

Time Required

90 minutes

Target Audience

- Developers

Learnings

Participants will walk away from the workshop with an introduction to:

- Understanding the difference between OTLP and file-based logging with OTel
- Understanding OTel Semantic Conventions and why they are needed for logging
- Using OTTL and OTTL Playground to build log parsing transforms
- Parsing JSON logs with OTTL
- Modifying the OpenTelemetry Collector Configuration
- Using the OpenTelemetry Receiver Creator on Kubernetes to dynamically inject log parsing
- Understanding and using OpenTelemetry Baggage
- Understanding and using OpenTelemetry log/span correlation
- Understanding and using native logging frameworks with OTel to do structured logging
- Using SQL Commenter to attach trace.id to SQL audit logs
- Using ES|QL to search logs
- Using ES|QL to parse logs at query-time
- Using Streams to setup ingest-time log processing