Logging with OpenTelemetry

This is a hands-on workshop showcasing various methods for working with OpenTelemetry logs using 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 configurations.

Time Required

90 minutes

Target Audience

- Developers

Learnings

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

- Using OTTL and OTTL Playground to build log parsing transforms
- Modifying the OpenTelemetry Collector Configuration to plumb OTTL
- Using the OpenTelemetry Receiver Creator on k8s to dynamically insert log parsing statements
- Parse JSON logs
- Understand and use OpenTelemetry Baggage
- Understand and use OpenTelemetry log/span correlation
- Understand and use native logging frameworks with OTel to do structured logging
- Employ SQL Commentor 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