Using the Splunk Log Observer

This course is designed for developers responsible for debugging their own applications, and for SREs responsible for troubleshooting performance issues. The Splunk Log Observer is built primarily for DevOps teams working on applications built on modern tech stacks (containerized micro-services). However, the course it can be taken by anyone who wants to view recent log data in a no-code environment.

This 1-virtual-day course describes how to use the tool to work with log data using the no-code user interface. You will learn to create, save, and share search filters; and to investigate the shape of your log data. You will analyze logs with aggregation functions and group by rules. And you will create rules to manipulate incoming data, as well as to generate synthetic metrics from log data.

All concepts are taught using lectures and scenario-based hands-on activities.

Course Topics

- View log data
- Describe how log data is parsed and structured in the tool
- Create filters for log data; save and reuse these filters
- Investigate the shape of log data with the Log Observer
- Analyze data with aggregation functions and group by rules
- Manage the data pipeline using rules
- Create Synthetic Metrics from Log Data

Course Prerequisites

Prior experience with Splunk Infrastructure Monitoring and/or Splunk APM is recommended.

Class Format

Instructor-led lecture with labs, delivered via virtual classroom or at your site

Course Objectives

Module 1 – Introduction

- Describe the "Three Pillars of Observability"
- Explain how Splunk navigates between the three data types
- Explain at a high level how Splunk collects each data type
- Explain what a no-code search is
- Describe some use cases for the Log Observer

Module 2 – Log Observer Basics

- Use the Log Observer to view trends in logs over time
- Use an aggregation function to summarize log data
- Browse fields and top values for logs
- Create a set of filters from field data
- Save filter sets
- Change the time range for logs displayed
- Describe the relationship between the four parts of the Log Observer Interface

Module 3 – Advanced Searching

- Add multiple search filters using field values and keywords
- Create and tag Saved Queries
- Create visualizations from aggregate log data
- Segment visualization using group by
- Use search time rules to temporarily transform incoming data
- View and configure Live Tail mode
- Restrict time windows for viewing log data in various ways

Module 4 – Managing Data Pipelines

- Describe the data processing pipeline and data indexing
- Explain some use cases for data processing rules
- Describe the rule types
- Differentiate between index-time and search-time rules
- Add a rule to the pipeline or edit an existing rule
- Create synthetic metrics from log data
- Create rules to determine which data is indexed vs being archived (Infinite Logging)

Module 5 – Getting Data In

- Explain field types in the Log Observer
- Describe the various ways to bring log data into Splunk Observability
- Name some of the ways that log data is enriched
- Differentiate between log messages and metadata
- Describe how metadata is stored and accessed on log messages

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all of Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/goto/education

To contact us, email education_AMER@splunk.com