Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Using Splunk Log Observer Connect

CODE:	LENGTH:	PRICE:
SPL_USLOC	8 Hours (1 day)	Request Price

Description

This course is designed for developers responsible for debugging their own applications, and for SREs responsible for troubleshooting performance issues. Splunk Log Observer Connect is built primarily for DevOps teams working on applications built on modern tech stacks (containerized microservices) and who need to explore logs from Splunk Cloud Platform or Splunk Enterprise in Splunk Observability Cloud. However, the course can be taken by anyone who wants to view recent log data in a no-code environment.
This course describes how to use the tool to work with log data using the no-code user interface. Learn to create, save, and share search filters, and to investigate Splunk Cloud/Enterprise logs in context with correlated metrics and traces. Learn to add log messages to dashboards. Analyze logs with aggregation functions and group by rules. All concepts are taught using lectures and scenario-based hands-on activities

Objectives

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 Log Observer Connect
▪ Analyze data with aggregation functions and group by rules
▪ Describe Log Observer Connect setup

Audience

Developer
Administrators

Prerequisites

Introduction to Splunk Observability (eLearning)
▪ Introduction to Splunk Log Observer Connect (eLearning)
▪ Basic knowledge of navigating and visualizing metrics in Splunk Observability Cloud

Programme

Course Objectives Module 1 – Explore Splunk Log Observer Connect
▪ Determine how to navigate between types of telemetry data
▪ Define the term "no-code search"
▪ Describe some use cases for Log Observer Connect
Module 2 – Log Observer Connect Basics
▪ 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 user interface
Module 3 – Advanced Searching
▪ Add multiple search filters using field values and keywords
▪ Create and tag Saved Queries
▪ Create log views
▪ Create visualizations from aggregate log data

▪ Save logs to dashboards
▪ Segment visualization using Group by
▪ Restrict time windows for viewing log data in various ways
Module 4 – Set up Log Observer Connect
▪ Get data from the Splunk platform
▪ Explain field types in Log Observer Connect
▪ Name some of the ways that log data is enriched
▪ Differentiate between log messages and metadata

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

This training is also available as onsite training. Please contact us to find out more.