SPLK-CVAL: Comparing Values

Course Code: SPLK-CVAL
Duration: 1 day
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

This three-hour course is for power users who want to learn how to compare field values using eval functions and eval expressions. Topics will focus on using the comparison and conditional functions of the eval command, and using eval expressions with the fieldformat and where commands.

SKILLS COVERED

- Please refer to course overview.

WHO SHOULD ATTEND?

Search Experts Knowledge Managers

PREREQUISITES

To be successful, students should have a solid understanding of the following:

- How Splunk works
- Creating Search queries

MODULES

Module 1: Using eval to Compare

- Understand the eval command
- Explain evaluation functions
- Identify and use comparison and conditional functions
- Use the fieldformat command to format field values

Module 2: Filtering with where

- Use the where command to filter results
- Use wildcards with the where command
- Filter fields with the information functions, isnull and isnotnull

Module 3: Using Fields in Searches

- Use fields correctly in basic searches
- Use fields with operators
- Use the rename command
- Use the fields command to improve search performance

Module 4: Comparing Temporary versus Persistent Fields

- Differentiate between temporary and persistent fields
- Create temporary fields with the eval command
- Extract temporary fields with the erex and rex commands

Module 5: Enriching Data

- Understand how fields from lookups, calculated fields, field aliases, and field extractions enrich data

END OF PAGE