Multivalue Fields

(SP-SMV)

COURSE OVERVIEW

This course is part of the following Certifications:

- Splunk Core Certified Advanced Power User

PREREQUISITES

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

- How Splunk works
- Creating search queries

COURSE OBJECTIVES

- What are Multivalue Fields
- Creating Multivalue Fields
- Evaluating Multivalue Fields
- Analyzing Multivalue Fields

Multivalue Fields

(SP-SMV)

COURSE OUTLINE

Topic 1 - What are Multivalue Fields?

- Understand multivalue fields
- Define self-describing data
- Understand how JSON data is handled in Splunk
- Use the spath command to interpret self-describing data
- Use the mvzip and mvexpand commands to manipulate multivalue fields
- Convert single-value fields to multivalue fields with specific commands and functions

Topic 2 - Creating Multivalue Fields

- Creating multivalue fields with the makemv command and the split function of the eval command

Topic 3 - Evaluating Multivalue Fields

- Use the mvcount, mvindex, and mvfilter eval functions to evaluate multivalue fields

Topic 4 - Manipulating Multivalue Data

- Use the mvsort, mvzip, mvjoin, mvmap, and mvappend eval functions and the mvexpand command to analyze multivalue data