Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

Multivalue Fields

CODE:	LENGTH:	PRICE:
SPL_SMF	0.96 Hours (0.12 days)	kr5,075.00

Description

This three-hour course is for power users who want to become experts on searching and manipulating multivalue data. Topics will focus on using multivalue eval functions and multivalue commands to create, evaluate, and analyze multivalue data.

Objectives

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

Audience

Search Experts Knowledge Managers

Prerequisites

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

- How Splunk works
- Creating Search queries

Programme

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 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 mvsotr, mvzip, mvjoin, mvmap, and mvappend eval functions and the mvexpand command to analyze multivalue data

Further Information

Individuals who enroll in this class will also be enrolled in an (eLearning with Labs) component. Completion of labs and quizzes is

required in order to receive proof of completion.

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.