email : techcenter@trainocate.com.my
contact : +603-2281-1111

SPLK-WTIME: Working with Time

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

OVERVIEW

This three-hour course is for power users who want to become experts at using time in searches. Topics will focus on searching and formatting time in addition to using time commands and working with time zones.

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
- The eval command

MODULES

Module 1: Searching with Time

- Understand the_time field and timestamps
- View and interact with the event Timeline
- Use the earliest and latest time modifiers
- Use the bin command with the _time field

Module 2: Formatting Time

- Use various date and time eval functions to format time

Module 3: Using Time Commands

- Use the timechart command
- Use the timewrap command

Module 4: Working with Time Zones

- Understand how time and timezones are represented in your data
- Determine the time zone of your server
- Use strftime to correct timezones in results

END OF PAGE