JSM

Splunk Fundamentals 1

Duration – 3 Days

Introduction:

- This course teaches you how to search and navigate in Splunk to create reports and dashboards, both using Splunk's searching and reporting commands and using the product's interactive Pivot tool. Scenario-based examples and hands-on challenges will enable you to create robust searches, reports, and charts.

Course Objectives

- **Module 1 – What is Splunk?**
- § Splunk components
- § Installing Splunk
- § Getting data into Splunk
- **Module 2 – Introduction to Splunk's User Interface**
- § Understand the uses of Splunk
- § Define Splunk Apps
- § Customizing your user settings
- § Learn basic navigation in Splunk
- **Module 3 – Basic Searching**
- § Run basic searches
- § Use auto complete to help build a search
- § Set the time range of a search
- § Identify the contents of search results
- § Refine searches
- § Use the timeline
- § Work with events
- § Control a search job
- § Save search results
- **Module 4 – Using Fields in Searches**
- § Understand fields
- § Use fields in searches
- § Use the fields sidebar
- **Module 5 – Search Language Fundamentals**
- § Review basic search commands and general search practices
- § Examine the search pipeline
- § Specify indexes in searches
- § Use autocomplete and syntax highlighting
- § Use the following commands to perform searches:

- tables
- rename
- fields
- dedup
- sort

- **Module 6 – Using Basic Transforming Commands**
- § The top command
- § The rare command
- § The stats command
- **Module 7 – Creating Reports and Dashboards**
- § Save a search as a report
- § Edit reports
- § Create reports that include visualizations such as charts and tables
- § Create a dashboard
- § Add a report to a dashboard
- § Edit a dashboard
- **Module 8 – Datasets and the Common Information Model**
- § Naming conventions
- § What are datasets?
- § What is the Common Information Model (CMI)?
- **Module 9 – Creating and Using Lookups**
- § Describe lookups
- § Create a lookup file and create a lookup definition
- § Configure an automatic lookup
- **Module 10 – Creating Scheduled Reports and Alerts**
- § Describe scheduled reports
- § Configure scheduled reports
- § Describe alerts
- § Create alerts
- § View fired alerts
- **Module 11 - Using Pivot**
- § Describe Pivot
- § Understand the relationship between data models and pivot
- § Select a data model object
- § Create a pivot report
- § Create an instant pivot from a search
- § Add a pivot report to a dashboard