Creating Knowledge Objects

This three-hour course is for knowledge managers who want to learn how to create knowledge objects for their search environment using the Splunk web interface. Topics will cover types of knowledge objects, the search-time operation sequence, and the processes for creating event types, workflow actions, tags, aliases, search macros, and calculated fields.

Course Topics

- Knowledge Objects and Search-time Operations
- Creating Event Types
- Using Event Type Builder
- Creating Workflow Actions
- Creating Tags and Aliases
- Creating Search Macros

Prerequisite Knowledge

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

- How Splunk works
- Knowledge objects

Course Format

Instructor-led or eLearning

Course Objectives

Topic 1 – Knowledge Objects & Search-time Operations

- Understand role of knowledge objects for enriching data
- Define search-time operation sequence

Topic 2 – Creating Event Types

- Define event types
- Create event types using three methods
- Tag event types
- Compare event types and reports

Topic 3 – Creating Workflow Actions

- Identify what are workflow actions
- Create a GET, POST, and search workflow action
- Test workflow actions

Topic 4 – Creating Tags and Aliases

- Describe field aliases and tags
- Create field aliases and tags
- Search with field aliases and tags

Topic 5 – Creating Search Macros

- Explain search macros
- Create macros with and without arguments
- Validate macro arguments
- Use and preview macros at search time
- Create and use nested macros
- Use macros with other knowledge objects

Topic 6 – Creating Calculated Fields

- Explain calculated fields
- Create a calculated field
- Use a calculated field in search

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/education

To contact us, email Education_AMER@splunk.com

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

Contact sales