splunk>

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
- Create Event Types
- Create Workflow Actions
- Create Tags and Aliases
- Create Search Macros
- Create Calculated Fields

Prerequisite Knowledge

To be successful, students should have completed the following courses:

- Search Under the Hood
- Multivalue Fields

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 – Create Event Types

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

Topic 3 – Create Workflow Actions

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

Topic 4 – Create Tags and Aliases

- Describe field aliases
- Create field aliases
- Search with field aliases
- Define tags
- Create and view tags
- Search with tags
- Manage tags

Topic 5 – Create Search Macros

- Define macros
- Create macros with and without arguments
- Validate macro arguments
- Use and preview macros at search time
- Use nested macros
- Use macros with other knowledge objects
- Use tags/event types with macros
- Create macros: considerations

Topic 6 – Create Calculated Fields

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

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