splunk>

Advanced Searching & Reporting with Splunk

This 3 virtual-day course focuses on more advanced search and reporting commands. Scenario-based examples and hands-on challenges enable users to create robust searches, reports, and charts. Students are coached step by step through complex searches to produce final results. Major topics include optimizing searches, additional charting commands and functions, formatting and calculating results, correlating events, and using combined searches and subsearches.

Course Topics

- Using Search Efficiently
- More Search Tuning
- Manipulating and Filtering Data
- Working with Multivalue Fields
- Using Advanced Transactions
- Working with Time
- Combining Searches
- Using Subsearches

Course Prerequisites

- Required
  - Splunk Fundamentals 1
  - Splunk Fundamentals 2
  - Splunk Fundamentals 3
- Highly recommended: at least 6 months experience with the Splunk search language

Class Format

Instructor-led lecture with labs, delivered via virtual classroom or at your site.

Course Objectives

Module 1 – Using Search Efficiently

- Review search architecture
- Understand how the components of a bucket (.tsidx and journal.gz files) are used
- How bloom filters are used to improve search speed
- Describe the parts of a search string
- Understand the use of centralized vs. distributable commands
- Create better searches

Module 2 – More Search Tuning

- Understand how segmenters are used in Splunk
- Use lispy to reduce the number of events read from disk

Module 3 – Manipulating and Filtering Data

- Divide search results into different groups, based on values in a specified field, using the bin command
- Regroup fields of search results using untable and xyseries
- Create a template for performing additional processing on a set of related fields using foreach

Module 4 – Working with Multivalue Fields

- Use multivalue eval functions to analyze and format data
- Use the makemv command to convert a single value into a multivalue field
- Use the mvexpand command to create separate events for each value in a multivalue field

Module 5 – Using Advanced Transactions

- Find events logged before or after a particular event occurs
- Compare complete vs. incomplete transactions
- Analyze transactions

Module 6 – Working with Time

- Use time modifiers
- Search for events using custom time ranges and time windows
- Display and use using relative dates
- Use custom time ranges in multiple subsearches

Module 7 – Combining Searches

- Use the append and appendcols commands (and know the differences)
- Use join and union (and when not to use them)

Module 8 – Using Subsearches

- Use subsearches to provide filtering and other information to a main search
- Know when NOT to use subsearches
- Troubleshoot subsearches

Module 9 – Some Extra Tips

- Describe the use of regular expressions
- Provide some guidance on using lookups
- Provide miscellaneous optimization tips

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

To contact us, email Education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
270 Brannan Street
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com