Search Under the Hood

This eLearning course gives students additional insight into how Splunk processes searches. Students will learn about Splunk architecture, how components of a search are broken down and distributed across the pipeline, and how to troubleshoot searches when results are not returning as expected.

Course Topics

- Understanding Splunk architecture
- Understanding how search terms are tokenized
- Using streaming and non-streaming commands
- Using troubleshooting commands and functions

Prerequisite Knowledge

Recommended:

Intro to Splunk eLearning course

Required:

none

Course Format

eLearning

Course Objectives

Topic 1 – Investigating Searches

- Use the Search Job Inspector to examine how a search was processed and troubleshoot performance
- Use SPL commenting to help identify and isolate problems

Topic 2 – Splunk Architecture

- Understand the role of search heads, indexers, and forwarders in a Splunk deployment
- Understand how the components of a bucket (.tsidx and journal.gz files) are used
- Understand how bloom filters are used to improve search speed

Topic 3 – Streaming and Non-Streaming Commands

- Describe the parts of a search string
- Understand the use of centralized vs. distributable commands
- Create more efficient searches

Topic 4 – Breakers and Segmentation

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

Topic 5 – Commands and Functions for Troubleshooting

- Using the fieldsummary command
- Using the makeresults command
- Using informational functions with the eval command
  - the isnull function
  - the typeof function

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