splunk>

Enriching Data with Lookups

This three-hour course is for knowledge managers who want to use lookups to enrich their search environment. Topics will introduce lookup types and cover how to upload and define lookups, create automatic lookups, and use advanced lookup options. Additionally, students will learn how to verify lookup contents in search and review lookup best practices.

Course Topics

- What is a Lookup?
- Create a Lookups
- Geospatial Lookups
- External Lookups
- KV Store Lookups
- Best Practices for Lookups

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 – What is a Lookup?

- Define a lookup and the default lookup types
- Lookups and the search-time operation sequence

Topic 2 – Create Lookups

- Describe lookups at search time
- Use file-based lookups
- Examine a CSV lookup file
- Create (upload, define, configure) a lookup
- Apply advanced lookup options
- Create and use an automatic lookup at search

Topic 3 – Geospatial Lookups

- Describe the use of geospatial lookups
- Examine KML/KMZ geospatial lookup files
- Add a geospatial lookup file
- Define a geospatial lookup

Topic 4 – External Lookups

- Define the use of external lookups
- Examine an external_lookup.py lookup script
- Configure external lookups

Topic 5 – KV Store Lookups

- Define the use of KV Store lookups
- Identify the steps to set up a KV Store lookup
- Examine the KV Store lookups collections.conf file

- Create a KV Store lookup definition
- Identify options for populating a KV Store lookup
- Compare file-based CSV lookups to KV Store lookups

Topic 6 – Best Practices for Lookups

- Various best practices for using lookups

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