Using the Splunk REST API

This 9-hour course is designed for application developers and administrators that want to utilize the Splunk REST API. In this course, you will learn how to make REST API requests and parse the server responses. Major topics include authentication, server administration, and implementation of a variety of search types. You will also ingest data using the HTTP Event Collector and manage application data using the Key-Value Store.

Course Objectives

- Describe the Splunk REST API
- Manage servers and knowledge objects
- Execute a search and retrieve results
- Ingest events using the HTTP Event Collector
- Use the Key-Value Store to manage data

Prerequisite Knowledge

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

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration
- Python, JavaScript, or similar scripting languages

Course Format

Instructor-led lecture with lab exercises. Delivered via virtual classroom or at your site.

Course Topics

Topic 1 – Splunk REST API

- Introduce REST
- Review HTTP requests
- Describe the Splunk REST API
- Discuss authentication methods

Topic 2 – Response Data

- Review HTTP responses
- Describe the Atom specification
- Demonstrate how to retrieve JSON
- Explain how to parse a response

Topic 3 – Administration APIs

- Introduce the administration APIs
- Update configuration files
- Work with indexes
- Manage users

Topic 4 – Namespaces and Access Control

- Introduce namespaces
- Explain namespace use cases
- Implement access control

Topic 5 – Search

- Identify search components
- Review search best practices
- Create a search and retrieve results
- Discuss oneshot searches

Topic 6 – Advanced Search

- Utilize real-time searches
- Summarize export searches
- Construct saved searches
- Understand search job management

Topic 7 – HTTP Event Collector

- Describe the HTTP Event Collector
- Explain token management
- Explore data ingestion
- Implement data acknowledgement

Topic 7 – Key-Value Store

- Examine the Key-Value Store
- Define and manage a collection
- Create and manage records

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