splunk>

Developing with Splunk's REST API

This nine hour course teaches you to use the Splunk REST API to accomplish tasks on a Splunk server. In this course, you will use curl and Python to send requests to Splunk REST endpoints and will learn how to parse the results. The course will show you how to create a variety of objects in Splunk, how to work with and apply security to Splunk objects, issue different types of searches, and ingest data.

Course Topics

- Introduction to the Splunk REST API
- Namespaces and Object Management
- Parsing Output
- Oneshot Searching
- Normal and Export Searching
- Advanced Searching and Job Management
- Working with Indexes
- Using the HTTP Event Collector
- Course Wrap-Up (includes the SPL rest command)

Course Prerequisites

- Splunk Fundamentals 1
- Splunk Fundamentals 2
- Splunk Data Administration recommended but not required

Class Format

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

Course Objectives

Module 1 – Introduction to the Splunk REST API

- Use the proper case in searches
- Introduce the Splunk development environment and its REST endpoints
- Know to which Splunk server you should be connected to accomplish a desired task
- Authenticate with a Splunk server, with and without a session

Module 2 – Namespaces and Object Management

- Understand how a namespace affects access to objects
- Use the servicesNS node and a namespace to access objects
- Understand how the sharing level and access control lists affect access to objects
- Modify the sharing level and the permissions on an object

Module 3 – Parsing Output

- Understand the general structure of Atom-based output
- Format Atom-based JSON output

Module 4 – Oneshot Searching

- Review search language syntax and search best practices
- Execute a oneshot search
- Execute an export search
- Get search results

Module 5–Normal and Export Searching

- Identify types of searches
- Create normal and export searches
- Get:
  - Search results
  - Search job status and other search job properties

Module 6 – Advanced Searching and Job Management

- Executing a real time search
- Working with large results sets
- Working with saved searches
- Managing search jobs

Module 7 – Working with Indexes

- List Splunk indexes
- Get information about an index
- Create Splunk indexes
- Delete Splunk indexes

Module 8 – Using the HTTP Event Collector (HEC)

- Create and use HEC tokens
- Input data using HEC endpoints
- Get indexer event acknowledgements

Module 9– Using the rest Command

- Use the SPL rest command
- Final notes

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