Developing with the Splunk REST API

This 9-hour course is for developers who want to use the Splunk REST API to interact with Splunk servers. In this course, use curl and Python to send requests to Splunk REST endpoints and learn how to parse and use the results. Create a variety of objects in Splunk, learn how to change properties, work with and apply security to Splunk objects, run different types of searches and parse its results, ingest data using the HTTP Event Collector and manipulate collections and KV Stores.

Course Topics

- Introduction to the Splunk REST API
- Namespaces and Object Management
- Parsing Output
- Oneshot Searches
- Normal and Export Searches
- Advanced Searching and Job Management
- Working with KV Stores
- Using the HTTP Event Collector (HEC)

Prerequisite Knowledge

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

- Splunk Fundamentals 1 and 2

Or the following single-subject courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Working with Time
- Statistical Processing
- Search Under the Hood
- Introduction to Knowledge Objects

Students should also understand the following courses:

- Splunk Enterprise Data Administration (Recommended)

Course Format

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

Course Objectives

Module 1 – Introduction to the Splunk REST API

- Introduce the Splunk development environment and its REST endpoints
- Connect to the appropriate Splunk server to accomplish a desired task
- Authenticate with a Splunk server, with and without a session

Module 2 – Namespaces and Object Management

- Understand general CRUD with the REST API
- Identify 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
- Use the `rest` command.

Module 3 – Parsing Output

- Understand the general structure of Atom-based output
- Format Atom-based XML and JSON output
- Write code that uses the API and parse responses

Module 4 – Oneshot Searches

- Review search language syntax and search best practices
- Execute oneshot searches
- Get search results and parse them

Module 5 – Normal and Export Searches

- Identify types of searches
- Execute normal and export searches
- Get search results, job status and search job properties.

Module 6 – Advanced Searching and Job Management

- Execute real-time searches
- Work with large result sets
- Work with saved searches
- Manage search jobs

Module 7 – Working with KV Stores

- Define the function of a KV Store
- Define collections and records
- Perform CRUD operations on collections and records

Module 8 – Using the HTTP Event Collector (HEC)

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

Appendix – Useful Admin REST APIs

- Get system information
- Manage Splunk configuration files
- Manage Indexes

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