

Using the Splunk REST API


Summary

This course is for application developers and administrators.


This 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.


Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
 - Splunk Enterprise System Administration
 - Splunk Enterprise Data Administration
- Additional courses and/or knowledge in these areas are also highly recommended:
 - Python, JavaScript, or other scripting languages

**Format:**

- Instructor-led

**Instructor-led Duration:** 9 Hours

**Audience:**

- Administrators
- Engineers

Course Outline

Module 1 – Splunk REST API

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

Module 2 – Response Data

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

Module 3 – Administration APIs

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

Module 4 – Namespaces and Access Control

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

Module 5 – Search

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

Module 6 – Advanced Search

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

Module 7 – HTTP Event Collector

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

Module 8 – Key-Value Store

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

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit <http://www.splunk.com/education>.

To contact us, email education@splunk.com.

