Using the Splunk REST API (DSRAPI)

Course Content

Course Description:

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:

Upon successful completion of this course, students will be able to:

- 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

Prerequisites:

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

Splunk Enterprise System Administration (SESA), Splunk Enterprise Data Administration (SEDA), and Python, JavaScript, or similar scripting languages.

Target Audience:

Application developers and administrators.

Topics:

Lesson 1: Splunk REST API
- Introduce REST
- Review HTTP requests
- Describe the Splunk REST API
- Discuss authentication methods

Lesson 2: Response Data
- Review HTTP responses
- Describe the Atom specification
- Demonstrate how to retrieve JSON
- Explain how to parse a response

Lesson 3: Administration APIs
- Introduce the administration APIs
- Update configuration files
- Work with indexes
- Manage users

Lesson 4: Namespaces and Access Control
- Introduce namespaces
- Explain namespace use cases
- Implement access control

Lesson 5: Search
- Identify search components
- Review search best practices
- Create a search and retrieve results
- Discuss oneshot searches

Lesson 6: Advanced Search
- Utilize real-time searches
- Summarize export searches
- Construct saved searches
- Understand search job management

Lesson 7: HTTP Event Collector
- Describe the HTTP Event Collector
- Explain token management
- Explore data ingestion
- Implement data acknowledgement

Lesson 8: Key-Value Store
- Examine the Key-Value Store
- Define and manage a collection
- Create and manage records

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535