Using the Splunk REST API

(SP-DSRAPI)

COURSE OVERVIEW

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.

PREREQUISITES

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

• Splunk Enterprise System Administration (SESA)

• Splunk Enterprise Data Administration (SEDA)

• Python, JavaScript, or similar scripting languages

WHO SHOULD ATTEND

• Application developers and administrators.

COURSE OBJECTIVES

• Describe the Splunk REST API

• Manage servers and knowledge objects

• Execute a search and retrieve results

COURSE OUTLINE

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

Using the Splunk REST API

(SP–DSRAPI)

COURSE OUTLINE

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 8 – Key-Value Store

• Examine the Key-Value Store

• Define and manage a collection

• Create and manage records