splunk>

Developing with Splunk's Java and Python SDKs

This nine-hour course teaches you to use Splunk's REST API and Java and Python SDKs to bring new data into Splunk, remotely create and interact with Splunk objects such as ad-hoc and saved searches, and more. Learn to interact directly with the Splunk REST API, and also learn best practices for development—when are the SDKs the right choice, vs. REST, vs. other Splunk built-in tools.

Course Topics

- Exploring the REST API and SDKs
- Connection and authentication
- Object management and simple searching
- Advanced searching
- Handling search jobs and results
- Writing data to Splunk

Course Prerequisites

Using Splunk, Splunk Architecture Overview
Searching and Reporting with Splunk strongly recommended

Class Format

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

Course Objectives

Lesson 1 – Overview

- Understand the REST API and Splunk SDKs
- Identify Other Splunk development tools
- Use REST endpoints in simple scripts
- Understand the User/App context

Lesson 2 – Exploring the REST API and SDKs

- Install the Java SDK
- Install the Python SDK
- Explore SDK packages

Lesson 3 – Connection and Authentication

- Understand connection and authentication
- Understand the authentication process
- Use authentication tokens for multi-step operations
- Understand connection operations

Lesson 4 – Object Management

- List Splunk objects
- Create and edit Splunk objects

Lesson 5 – Basic Searching

- Understand basic search language syntax and search best practices
- Execute a search using the oneshot method
- Retrieve search results and display them on screen

Lesson 6 – Advanced Searching

- Identify types of searches
- Create normal, export, and real-time searches
- Create and run a saved search

Lesson 7 – Search Jobs and Results

- Managing jobs
- Traversing large result sets
- Count and Offset management
- Handling real-time jobs
- Managing Alerts

Lesson 8 – Writing Data to Splunk

- Create and manage indexes
- Identify best practices for writing data
- Use Input classes to add data to indexes
- Use direct input methods to add data to indexes

Splunk Education Tracks

User: For all day-to-day Splunk users including customer support staff, developers, systems administrators and management.

Administrator: For administrators of Splunk itself. (Administrators of other systems who will just be using Splunk should take the User track.)

Architect: For architects who will be designing Splunk deployments, including architects on staff at customer deployments as well as partner professional services personnel.

Developer: For developers who will integrate, customize and extend Splunk using its XML templates and advanced configuration bundling.

Support Engineer: For Splunk OEM and channel partner support staff who will be providing first line support for Splunk.

Tracks	User	Administrator	Architect	Developer	Support Engineer
Using Splunk	✓	✓	✓	✓	✓
Searching and Reporting with Splunk	✓		✓	✓	✓
Administrating Splunk		✓	✓		✓
Advanced Splunk Administration		✓	✓		✓
Architecting and Deploying Splunk			✓		✓
Developing Apps with Splunk			✓	✓	✓
Splunk Architect Certification Lab			✓		
Supporting Splunk					✓

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.
250 Brannan
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com