splunk>

Automation Using the REST and SignalFlow APIs

Splunk IM exposes a comprehensive API that allows you to automate any action that can be done using the User Interface. This 2-day virtual course provides the foundation for you to use the API to automate bulk actions such as the creation of charts, dashboards, and alerts. See how to programmatically perform computations that can be used in charts and detectors or streamed in real-time. Use the API to manage Splunk IMteams.

Learn the concepts and apply the knowledge through discussions and hands-on activities.

Course Topics

- Using the SignalFlow API to Perform Computations
- Stream/extract Raw and Processed Data from Splunk IM
- Manage Splunk IM Teams
- Manage Charts, Dashboards and Dashboard Groups Using the REST API
- Manage Detectors Using the REST API

Prerequisite Knowledge

Required:

- Using Splunk Infrastructure Monitoring

Course Format

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

Course Objectives

Module 1 – Overview of the Splunk IM API

- Describe the function of the API
- Describe the API endpoints

Module 2 – Streaming Computations Using SignalFlow

- Use the SignalFlow CLI
- Use the data() function to stream metrics
- Use the detect() function to define detectors

Module 3 – Streaming Raw and Processed Data

- Choose when to use WebSocket connection vs HTTP API for streaming
- Execute SignalFlow computations
- Describe the types of messages emitted by streaming computation
- Stream/extract raw and processed data from the Splunk IM service

Module 4 – Manage Splunk IM Teams

- Describe the use of teams
- Create teams
- Add/remove members to/from teams
- Update teams

Module 5 – Automate Chart and Dashboard Management

- Create, modify, and delete charts
- Create detectors to monitor issues of interest

Module 6 – Automate Detector Management

- Create detectors
- Update, delete detectors
- Mute notifications
- Clear incidents

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