Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Developing with Splunk's REST API 9.0

CODE:	LENGTH:	PRICE:
SPL_DWSRA90	16 Hours (2 days)	€1,000.00

Description

This nine hour course is for developers who want to use the Splunk REST API to interact with Splunk servers. In this course, you will use curl and Python to send requests to Splunk REST endpoints and learn how to parse and use the results. Create a variety of objects in Splunk, learn how to change properties, work with and apply security to Splunk objects, run different types of searches and parse its results, ingest data using the HTTP Event Collector and manipulate collections and KV Stores.

Objectives

- Introduction to the Splunk REST API
- Namespaces and Object Management
- Parsing Output
- Oneshot Searches
- Normal and Export Searches
- Advanced Searching and Job Management
- Working with KV Stores
- Using the HTTP Event Collector (HEC)

Prerequisites

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

- Splunk Fundamentals 1
- Splunk Fundamentals 2

OR the following single-subject courses:

- What Is Splunk?
- Intro to Splunk
- Using Fields
- Working with Time
- Statistical Processing
- Search Under the Hood
- Introduction to Knowledge Objects

Students should also have completed the following course:

- Splunk Enterprise Data Administration (recommended)

Programme

Module 1 – Introduction to the Splunk REST API

- Introduce the Splunk development environment and its REST endpoints
- Connect to the appropriate Splunk server to accomplish a desired task
- Authenticate with a Splunk server, with and without a session

Module 2 – Namespaces and Object Management

- Understand general CRUD with the REST API
- Identify how a namespace affects access to objects
- Use the servicesNS node and a namespace to access objects
- Understand how the sharing level and access control lists affect access to objects
- Modify the sharing level and the permissions on an object

Module 3 – Parsing Output

- Understand the general structure of Atom-based output
- Format Atom-based JSON output
- Write code that uses the API and parse responses

Module 4 – Oneshot Searches

- Review search language syntax and search best practices
- Execute a oneshot search
- Get search results

Module 5–Normal and Export Searches

- Identify types of searches
- Execute normal and export searches
- Get search results,job status and search job properties

Module 6 – Advanced Searching and Job Management

- Execute a real time search
- Work with saved searches
- Manage search jobs

Module 7 – Working with the KV Store

- Define the function of a KV Store
- Define collections and records
- Perform CRUD operations on collections and records

Module 8 – Using the HTTP Event Collector (HEC)

- Create and use HEC tokens
- Input data using HEC endpoints
- Get indexer event acknowledgements

Module 9 – Useful Admin REST APIs

- Get system information
- Manage Splunk configuration files
- Manage Indexes

Module 10 – Custom REST Endpoints

- Extending the Splunk REST API
- Publish your own endpoints
- Using custom REST API endpoints

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.