Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Developing with Splunk's REST API 8.1

CODE:	LENGTH:	PRICE:
SPL_DWSRA	2.96 Hours (0.37 days)	€1,000.00

Description

This nine hour course teaches you how to use the Splunk REST API to accomplish tasks interacting with Splunk servers. In this course, you will use curl and Python to send requests to Splunk REST endpoints and will learn how to parse and use the results. The course will show you how to create a variety of objects in Splunk, 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 Searching
- Normal and Export Searching
- Advanced Searching and Job Management
- Working with KV Stores
- Using the HTTP Event Collector

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

- Use the proper case in searches
- Introduce the Splunk development environment and its REST endpoints
- Know to which Splunk server you should be connected 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
- Understand 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
- Using the rest command

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
- Execute an export search
- Get search results

Module 5–Normal and Export Searching

- Identify types of searches
- Create normal and export searches
- Get:
- Search results
- Search job status and other search job properties

Module 6 – Advanced Searching and Job Management

- Executing a real time search
- Working with large results sets
- Working with saved searches
- Managing 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

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

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