



Enterprise Computing Solutions - Education Services

## TRAINING OFFERING

---

**Du kan nå oss här**

Kronborgsgränd 7, 164 46 Kista

Email: [edu.ecs.se@arrow.com](mailto:edu.ecs.se@arrow.com)

Phone: +46 8 555 188 00

| CODE:     | LENGTH:           | PRICE:      |
|-----------|-------------------|-------------|
| SPL_APUFS | 24 Hours (3 days) | kr32,000.00 |

## Description

This Advanced Power User Fast Start is :

- for power users who want to become experts on searching and manipulating multivalued data. Topics will focus on using multivalued eval functions and multivalued commands to create, evaluate, and analyze multivalued data.
- designed for power users who want to learn how to use lookups and subsearches to enrich their results. Topics will focus on lookup commands and explore how to use subsearches to correlate and filter data from multiple sources.
- for power users who want to improve search performance. Topics will cover how search modes affect performance, how to create an efficient basic search, how to accelerate reports and data models, and how to use the `tstats` command to quickly query data.
- for knowledge managers who want to use lookups to enrich their search environment. Topics will introduce lookup types and cover how to upload and define lookups, create automatic lookups, and use advanced lookup options. Additionally, students will learn how to verify lookup contents in search and review lookup best practices.
- designed for power users who want to learn best practices for building dashboards in the Dashboard Studio. It focuses on dashboard creation, including prototyping, the dashboard definition, layout types, adding visualizations, and dynamic coloring.
- designed for power users who want to learn best practices for building dashboards in the Dashboard Studio. It focuses on creating inputs, chain searches, event annotations, and improving dashboard performance.

## Objectives

### Course Topics

- Using Lookup Commands
- Adding a Subsearch
- Using the `return` Command
- What are Multivalued Fields
- Creating Multivalued Fields
- Evaluating Multivalued Fields
- Analyzing Multivalued Fields
- Optimizing Search
- Report Acceleration
- Data Model Acceleration
- Using the `tstats` Command
- What is a Lookup?
- Creating Lookups
- Geospatial Lookups
- External Lookups
- KV Store Lookups
- Best Practices for Lookups
- Dashboard Framework
- Prototyping
- Visualization Types
- Modifying the Source Code
- Dynamic Coloring
- Data Source Types
- Mock Data
- Event Annotations
- Adding Inputs

- Chain Searches

## Audience

Search Experts Knowledge Managers

## Prerequisites

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

- How Splunk works
- Knowledge objects
- Lookups
- Creating Search queries
- Creating reports and data models
- Data structure requirements for visualizations
- The dashboard definition

## Programme

### Module 1 : Leveraging Lookups and Subsearches (SSC)

Topic 1 – Using Lookup Commands

- Understand lookups
- Use the inputlookup command to search lookup files
- Use the lookup command to invoke field value lookups
- Use the outputlookup command to create lookups
- Invoke geospatial lookups in search

Topic 2 – Adding a Subsearch

- Define subsearch
- Use subsearch to filter results
- Identify when to use subsearch
- Understand subsearch limitations and alternatives

Topic 3 – Using the return Command

- Use the return command to pass values from a subsearch
- Compare the return and fields commands

### Module 02 : Multivalued Fields (SSC)

Topic 1 – What are Multivalued Fields?

- Understand multivalued fields
- Define self-describing data
- Understand how JSON data is handled in Splunk
- Use the spath command to interpret self-describing data
- Use mvzip and mvexpand commands to manipulate multivalued fields
- Convert single-value fields to multivalued fields with specific commands and functions

Topic 2 – Creating Multivalued Fields

- Creating multivalued fields with the makemv command and the split function of the eval command

Topic 3 – Evaluating Multivalued Fields

### Module 03 : Search Optimization (SSC)

Topic 1 – Optimizing Search

- Understand how search modes affect performance
- Examine the role of the Splunk Search Scheduler
- Review general search practices

Topic 2 – Report Acceleration

- Define acceleration and acceleration types
- Understand report acceleration and create an accelerated report
- Reveal when and how report acceleration summaries are created
- Search against acceleration summaries

Topic 3 – Data Model Acceleration

- Understand data model acceleration
- Accelerate a data model
- Use the datamodel command to search data models

## Topic 4 – Using the tstats Command

- Explore the tstats command
- Search acceleration summaries with tstats
- Search data models with tstats
- Compare tstats and stats

### **Module 04 : Enriching Data With Lookups (SSC)**

#### Topic 1 – What is a Lookup?

- Define a lookup and the default lookup types
- Lookups and the search-time operation sequence

#### Topic 2 – Creating Lookups

- Use file-based lookups at search time
- Create (upload, define, configure) a lookup
- Use an automatic lookup at search

#### Topic 3 – Geospatial Lookups

- Understand geospatial lookups and KMZ/KML files
- Add and define a geospatial lookup

#### Topic 4 – External Lookups

- Understand external lookups
- Explore the default lookups, external\_lookup.py
- Configure external lookups

#### Topic 5 – KV Store Lookups

- Introduce KV Store lookups
- Configure KV Store lookups
- Compare file-based CSV lookups to KV Store lookups

#### Topic 6 – Best Practices for Lookups

- Various best practices for using lookups

### **Module 05 : Intro To Dashboards (SSC)**

#### Topic 1 – Dashboard Framework

- Describe the dashboard definition
- Compare classic and dashboard studio dashboards
- Use dashboard best practices
- Manage views
- Use dashboard best practices

#### Topic 2 – Create a Prototype

- Describe dashboard workflows
- Compare layout types
- Identify layout fields
- Add visualizations

#### Topic 3 – Use Dynamic Coloring

- Describe dynamic coloring
- Contrast visualization types
- Set global time range parameters
- Apply dynamic coloring

### **Modules 06 : Dynamic Dashboards (SSC)**

#### Topic 1 – Selecting a Data Source

- Identify dataSources stanza fields
- Name search types
- Use a secondary data source

#### Topic 2 – Adding Inputs

- Identify types of inputs
- Describe how inputs work
- Create a dynamic input
- Add cascading inputs

#### Topic 3 – Improving Performance

- Identify performance improvement methods
- Use tstats and accelerated data models
- Create chain searches

- Set defaults

Topic 4 – Comparing Temporary versus Persistent Fields

- Differentiate between temporary and persistent fields
- Create temporary fields with the eval command
- Extract temporary fields with the erex and rex commands

Topic 5 – Enriching Data

- Understand how fields from lookups, calculated fields, field aliases, and field extractions enrich data

## Session Dates

| Date        | Location                | Time Zone | Language | Type                  | Guaranteed | PRICE       |
|-------------|-------------------------|-----------|----------|-----------------------|------------|-------------|
| 01 Jun 2026 | Virtual Classroom (CET) | CEDT      | English  | Instructor Led Online |            | kr32,000.00 |

## Ytterligare information

[Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.](#)