Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns unter

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: training.ecs.de@arrow.com
Phone: +49 (0)89 930 99 168

splunk>   Advanced Power User Fast Start

CODE:	LÄNGE:	PREIS:
SPL_APUFS	3 Tage	€3,000.00

Description

This Advanced Power User Fast Start is :

- for power users who want to become experts on searching and manipulating multivalue data. Topics will focus on using multivalue eval functions and multivalue commands to create, evaluate, and analyze multivalue 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, layouts 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.

Lernziel

Course Topics • Using Lookup Commands • Adding a Subsearch • Using the return Command • What are Multivalue Fields • Creating Multivalue Fields • Evaluating Multivalue Fields • Analyzing Multivalue 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

Zielgruppe

Search Experts Knowledge Managers

Voraussetzungen

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

Inhalt

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 : Multivalue Fields (SSC)   Topic 1 – What are Multivalue Fields?

- Understand multivalue 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 multivalue fields

- Convert single-value fields to multivalue fields with specific commands and functions
 Topic 2 – Creating Multivalue Fields

- Creating multivalue fields with the makemv command and the split function of the eval command
 Topic 3 – Evaluating Multivalue 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 ad 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

Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
30 Jan 2023	Virtual Classroom	CET	English	Instructor Led Online		€3,000.00
15 Mar 2023	Virtual Classroom	CET	English	Instructor Led Online		€3,000.00
22 May 2023	Virtual Classroom	CEDT	English	Instructor Led Online		€3,000.00
19 Jun 2023	Virtual Classroom	CEDT	English	Instructor Led Online		€3,000.00
20 Sep 2023	Virtual Classroom	CEDT	English	Instructor Led Online		€3,000.00
15 Nov 2023	Virtual Classroom	CET	English	Instructor Led Online		€3,000.00
29 Nov 2023	Virtual Classroom	CET	English	Instructor Led Online		€3,000.00

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.