



Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com
Phone: +420 597 488 811



Splunk Power User Fast Track

Kód:	DÉLKA:	CENA:
SPL_POWER-U	32 Hours (4 DENNÍ)	Kč bez DPH 99,800.00

Description

Cena školení je 4 000 EUR a bude přepočtena aktuálním kurzem v poslední den školení.

This course is for Splunk Power Users who want to become experts on the following Splunk topics : Working with Time :for power users who want to become experts at using time in searches. Topics will focus on searching and formatting time in addition to using time commands and working with time zones. Statistical Processing :to identify and use transforming commands and eval functions to calculate statistics on their data. Topics will cover data series types, primary transforming commands, mathematical and statistical eval functions, using eval as a function, and the rename and sort commands. Comparing Values :to learn how to compare field values using eval functions and eval expressions. Topics will focus on using the comparison and conditional functions of the eval command, and using eval expressions with the field format and where commands Result Modification :to use commands to manipulate output and normalize data. Topics will focus on specific commands for manipulating fields and field values, modifying result sets, and managing missing data. Additionally, students will learn how to use specific eval command functions to normalize fields and field values across multiple data sources. Correlation Analysis :to learn how to calculate co-occurrence between fields and analyze data from multiple datasets. Topics will focus on the transaction, append, appendcols, union, and join commands. Creating Knowledge Objects :to learn how to create knowledge objects for their search environment using the Splunk web interface. Topics will cover types of knowledge objects, the search-time operation sequence, and the processes for creating event types, workflow actions, tags, aliases, search macros, and calculated fields. Creating Field Extractions :to learn about field extraction and the Field Extractor (FX) utility. Topics will cover when certain fields are extracted and how to use the FX to create regex and delimited field extractions. Data Models :to learn how to create and accelerate data models. Topics will cover datasets, designing data models, using the Pivot editor, and accelerating data models.

Cíle

Working with Time Statistical Processing Comparing Values Result Modification Correlation Analysis Creating Knowledge Objects Creating Field Extractions Data Models

Vstupní znalosti

How Splunk works

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

Prerequisites can be obtain with free elearning :

What is Splunk (SSC) : https://www.splunk.com/en_us/training/courses/what-is-splunk.html

Intro to Splunk (SSC) : https://www.splunk.com/en_us/training/courses/intro-to-splunk.html

Using Fields (SSC) : https://www.splunk.com/en_us/training/courses/using-fields.html

Visualizations (SSC) : https://www.splunk.com/en_us/training/courses/visualizations.html

Intro to Knowledge Objects (SSC) : https://www.splunk.com/en_us/training/courses/intro-to-knowledge-objects.html

Search Under the Hood (SSC) : https://www.splunk.com/en_us/training/courses/search-under-the-hood.html

Or ask Arrow Education Team for Prerequisites Fast Start bundle (SPL_PREREQ)

Program

Understand the _time field and timestamps

View and interact with the Event Timeline

Use the earliest and latest time modifiers

Use the bin command with the _time field

Working with Time : Module 1 - Searching with Time

Module 2 - Formatting Time

Use various date and time eval functions to format time

Use the timechart command

Use the timewrap command

Module 3 - Using Time Commands

	Understand how time and timezones are represented in your data	
	Determine the time zone of your server	
	Use strftime to correct timezones in results	
Module 4 - Working with Time Zones	Statistical Processing :	
	Introduce data series	
	Explore the difference between single-series, multi-series, and time series data series	
Module 1 - What is a Data Series		Use the chart, timechart, top, rare, and stats commands to transform events into data tables
Module 2 - Transforming Data		
Module 3 - Manipulating Data with eval Command		
Understand the eval command		
Explore and perform calculations using mathematical and statistical eval functions		
Perform calculations and concatenations on field values		
Use the eval command as a function with the stats command		
		Module 4 - Formatting Data
		Understand the eval command
		Explain evaluation functions
Use the rename command		Identify and use comparison and conditional functions
Use the sort command		Use the fieldformat command to format field values
Comparing Values	Module 1 - Using eval to Compare	
	Use the where command to filter results	
	Use wildcards with the where command	
	Filter fields with the information functions, isnull and isnotnull	
Module 2 - Filtering with where	Result Modification	Module 1 - Manipulating Output
Convert a 2-D table into a flat table with the untable command		
Convert a flat table into a 2-D table with the xyseries command		
		Module 2 - Modifying Result Sets
Append data to search results with the appendpipe command		
Calculate event statistics with the eventstats command		
Calculate "streaming" statistics with the streamstats command		
Modify values to segregate events with the bin command		
		Module 3 - Managing Missing Data
Find missing and null values with the fillnull command		
		Module 4 - Modifying Field Values
Understand the eval command		
Use conversion and text eval functions to modify field values		
Reformat fields with the foreach command		
		Module 5 - Normalizing with eval
Normalize data with eval functions		
Identify eval functions to use for data and field normalization		
Correlation Analysis		Module 1 - Calculate Co-Occurrence Between Fields
Understand transactions		
Explore the transaction command		
		Module 2 - Analyze Multiple Data Sources
Understand subsearch		
Use the append, appendcols, union, and join commands to combine, analyze, and compare multiple data sources		
Creating Knowledge Objects		
		Understand role of knowledge objects for enriching data
		Define search-time operation sequence
Topic 1 – Knowledge Objects & Search-time Operations		
	Define event types	
	Create event types using three methods	Identify what are workflow actions
	Tag event types	Create a GET, POST, and search workflow action
	Compare event types and reports	Test workflow actions
Topic 2 – Creating Event Types	Topic 3 – Creating Workflow Actions	
	Describe field aliases and tags	
	Create field aliases and tags	
	▪ Search with field aliases and tags	
Topic 4 – Creating Tags and Aliases		Topic 5 – Creating Search Macros
Explain search macros		
Create macros with and without arguments		
Validate macro arguments		
Use and preview macros at search time		Explain calculated fields
Create and use nested macros		Create a calculated field
Use macros with other knowledge objects		Use a calculated field in search
		Topic 6 – Creating Calculated Fields
	Creating Field Extractions	
	Understand types of extracted fields and when they are extracted	
	Explore the Splunk Web Field Extractor (FX)	
Module 1 - Using the Field Extractor		

Identify basics of regular expressions (regex)
Understand the regex field extraction workflow
Edit regex for field extractions

Module 2 - Creating Regex Field Extractions

Identify delimited field values in event data
Understand the delimited field extraction workflow

Module 3 - Creating Delimited Field Extractions Data Models

Understand data models
Add event, search, and transaction datasets to data models
Identify event object hierarchy and constraints
Add fields based on eval expressions to transaction datasets

Module 1 - Introducing Data Model Datasets

Create a data model
Add root and child datasets to a data model
Add fields to data models
Test a data model
Define permissions for a data model
Upload/download a data model for backup and sharing

Module 2 - Designing Data Models

Identify benefits of using Pivot
Create and configure a Pivot
Visualize a Pivot
Save a Pivot
Use Instant Pivot
Access underlying search for Pivot

Module 3 - Creating a Pivot

Module 4 - Accelerating Data Models

Understand the difference between ad-hoc and persistent data model acceleration
Accelerate a data model
Describe the role of tsidx files in data model acceleration
Review considerations about data model acceleration

Zkoušky a certifikace

Certification : Splunk Core Certified Power User

Termíny školení

Termíny školení na vyžádání, [kontaktujte nás prosím](#)

Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)