Splunk Power User Fast Start

Dieser Kurs richtet sich an Splunk Power User, die Experten in den folgenden Splunk-Themen werden wollen:

Arbeiten mit Zeit :

für Power-User, die Experten im Umgang mit der Zeit in der Suche werden wollen. Die Themen konzentrieren sich auf die Suche und Formatierung der Zeit sowie auf die Verwendung von Zeitbefehlen und die Arbeit mit Zeitzonen.

Statistische Verarbeitung :

Identifizierung und Verwendung von Transformationsbefehlen und Eval-Funktionen zur Berechnung von Statistiken über ihre Daten. Die Themen umfassen Typen von Datenreihen, primäre Transformationsbefehle, mathematische und statistische eval-Funktionen, die Verwendung von eval als Funktion sowie die Befehle Umbenennen und Sortieren.

Werte vergleichen:

Sie lernen, wie man Feldwerte mit eval-Funktionen und eval-Ausdrücken vergleicht. Die Themen konzentrieren sich auf die Verwendung der Vergleichs- und Bedingungsfunktionen des eval-Befehls und die Verwendung von eval-Ausdrücken mit den Befehlen Feldformat und Wo.

Modifizierung von Ergebnissen:

Verwendung von Befehlen zur Manipulation von Ausgaben und zur Normalisierung von Daten. Die Themen konzentrieren sich auf spezifische Befehle zur Bearbeitung von Feldern und Feldwerten, zur Änderung von Ergebnismengen und zur Verwaltung fehlender Daten. Darüber hinaus lernen die Teilnehmer, wie sie spezifische eval-Befehlsfunktionen zur Normalisierung von Feldern und Feldwerten über mehrere Datenquellen hinweg verwenden können.

Korrelationsanalyse:

Die Teilnehmer lernen, wie man das gemeinsame Auftreten von Feldern berechnet und Daten aus mehreren Datensätzen analysiert. Die Themen konzentrieren sich auf die Befehle transaction, append, appendcols, union und join.

Erstellen von Wissensobjekten:

Die Teilnehmer lernen, wie sie mithilfe der Splunk-Webschnittstelle Wissensobjekte für ihre Suchumgebung erstellen können. Die Themen umfassen die Arten von Wissensobjekten, die Reihenfolge der Suchvorgänge und die Prozesse zur Erstellung von Ereignistypen, Workflow-Aktionen, Tags, Aliases, Suchmakros und berechneten Feldern.

Erstellen von Feldextraktionen:

Sie lernen etwas über Feldextraktion und das Dienstprogramm Field Extractor (FX). Es wird behandelt, wann bestimmte Felder extrahiert werden und wie man den FX verwendet, um Regex- und begrenzte Feldextraktionen zu erstellen.

Datenmodelle:

Sie lernen, wie Sie Datenmodelle erstellen und beschleunigen können. Die Themen umfassen Datensätze, den Entwurf von Datenmodellen, die Verwendung des Pivot-Editors und die Beschleunigung von Datenmodellen.

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

Zielgruppe
Der Kurs richtet sich an Splunk Power User.

Voraussetzungen
Um erfolgreich zu sein, sollten die Studierenden ein solides Verständnis der folgenden Punkte haben:

- Wie Splunk funktioniert
- Erstellen von Suchanfragen

Die Voraussetzungen können mit kostenlosem E-Learning erworben werden. Für den Zugriff auf die E-Learnings ist eine Registrierung bei Splunk erforderlich, falls noch kein Account existiert:

- What is Splunk (Video)
- Intro to Splunk
- Using Fields
- Visualizations
- Intro to Knowledge Objects
- Search Under the Hood

Kursziel
Certification: Splunk Core Certified Power User

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/**SPUF**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		**Preise zzgl. MwSt.**	
Termine in Deutschland		**4 Tage**	**€ 4.000,-**
Online Training		**4 Tage**	**€ 4.000,-**
Termin/Kursort		Kurssprache Deutsch	
19.05.-22.05.25	ONOnline	06.10.-09.10.25	HYMünchen
23.06.-26.06.25	ONOnline	06.10.-09.10.25	HYOnline
21.07.-24.07.25	HYMünchen	01.12.-04.12.25	HYMünchen
21.07.-24.07.25	HYOnline	01.12.-04.12.25	HYOnline
01.09.-04.09.25	ONOnline		

Stand 07.05.2025

ExperTeach

Splunk

Inhaltsverzeichnis

Splunk Power User Fast Start

Working with Time :
Module 1 - Searching with Time
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

Module 2 - Formatting TIme
Use various date and time eval functions to format time

Module 3 - Using Time Commands
Use the timechart command
Use the timewrap command

Module 4 - Working with Time Zones
Understand how time and timezones are represented in your data
Determine the time zone of your server
Use strftime to correct timezones in results

Statistical Processing :
Module 1 - What is a Data Series
Introduce data series
Explore the difference between single-series, multi-series, and time series data series

Module 2 - Transforming Data
Use the chart, timechart, top, rare, and stats commands to transform events into data tables

Module 3 - Manipulating Data with eval Command
Understand dthe 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
Use the rename command
Use the sort command

Comparing Values
Module 1 - Using eval to Compare
Understand the eval command
Explain evaluation functions
Identify and use comparison and conditional functions
Use the fieldformat command to format field values

Module 2 - Filtering with where
Use the where command to filter results
Use wildcards with the where command
Filter fields with the information functions, isnull and isnotnull

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

Topic 1 – Knowledge Objects & Search-time Operations
Understand role of knowledge objects for enriching data
Define search-time operation sequence

Topic 2 – Creating Event Types
Define event types
Create event types using three methods
Tag event types
Compare event types and reports

Topic 3 – Creating Workflow Actions
Identify what are workflow actions
Create a GET, POST, and search workflow action
Test workflow actions

Topic 4 – Creating Tags and Aliases
Describe field aliases and tags
Create field aliases and tags
▪ Search with field aliases and tags

Topic 5 – Creating Search Macros
Explain search macros
Create macros with and without arguments
Validate macro arguments
Use and preview macros at search time
Create and use nested macros
Use macros with other knowledge objects

Topic 6 – Creating Calculated Fields
Explain calculated fields
Create a calculated field
Use a calculated field in search

Creating Field Extractions
Module 1 - Using the Field Extractor
Understand types of extracted fields and when they are extracted
Explore the Splunk Web Field Extractor (FX)

Module 2 - Creating Regex Field Extractions
Identify basics of regular expressions (regex)
Understand the regex field extraction workflow
Edit regex for field extractions

Module 3 - Creating Delimited Field Extractions
Identify delimited field values in event data
Understand the delimited field extraction workflow

Data Models
Module 1 - Introducing Data Model Datasets
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 2 - Designing Data Models
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 3 - Creating a Pivot
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 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

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de