

Splunk - Developer Fast Start

Einführung in Dashboards: für Power-User, die Best Practices für die Erstellung und Bearbeitung von JSON-basierten Dashboards in Dashboard Studio erlernen möchten. Der Schwerpunkt liegt auf der Erstellung von Eingaben, der Bearbeitung von Dashboard-Quellcode, Kettensuchen, Ereignisanmerkungen und der Verbesserung der Dashboard-Leistung.

Dynamische Dashboards: für Power-User, die Best Practices für die Erstellung JSON-basierter, interaktiver Dashboards in Dashboard Studio erlernen möchten. Der Schwerpunkt liegt auf der Erstellung von Benutzereingaben, der Bearbeitung von Dashboard-Quellcode, Kettensuchen, Ereignisanmerkungen und der Verbesserung der Dashboard-Leistung.

Advanced Dashboards and Visualizations: richtet sich an fortgeschrittene Benutzer, die SplunkJS-basierte Dashboards und Formulare erstellen möchten. Es konzentriert sich auf die Erstellung von Dashboards, das Hinzufügen von Eingaben, die Verwendung von Event-Handlern und die Erstellung von Splunk Custom Visualizations.

Building Splunk Apps: konzentriert sich auf die Entwicklung von Splunk Enterprise-Apps. Es richtet sich an fortgeschrittene Benutzer, Administratoren und Entwickler, die Apps mit dem Splunk Web Framework erstellen wollen. Zu den Hauptthemen gehören die Planung der App-Entwicklung, die Erstellung von Datengeneratoren und Dateneingaben, die REST-API, Setup-Bildschirme, der KV Store und die App-Paketierung.

Developing with Splunk's REST API: für Entwickler, die die Splunk REST API nutzen wollen, um mit Splunk Servern zu interagieren. In diesem Kurs verwenden Sie curl und Python, um Anfragen an Splunk REST-Endpunkte zu senden und lernen, wie man die Ergebnisse analysiert und verwendet. Erstellen Sie eine Vielzahl von Objekten in Splunk, lernen Sie, wie Sie Eigenschaften ändern, mit Splunk-Objekten arbeiten und diese absichern, führen Sie verschiedene Arten von Suchen durch und analysieren Sie deren Ergebnisse, nehmen Sie Daten mit dem HTTP Event Collector auf und manipulieren Sie Sammlungen und KV-Speicher.

Kursinhalt

- Introduction to Dashboards
- Dynamic Dashboards
- Advanced Dashboards and Visualizations
- Building Splunk Apps

Voraussetzungen

Um erfolgreich zu sein, sollten die Teilnehmer ein solides Verständnis der folgenden Kurse haben:

- Was ist Splunk?
- Einführung in Splunk
- Felder verwenden
- Visualisierungen
- Nutzung von Lookups & Subsearches
- Korrelationsanalyse
- Suche unter der Haube
- Einführung in Wissensobjekte
- Erstellen von Wissensobjekten
- Erstellen von Feldextraktionen
- Anreicherung von Daten mit Lookups
- Einführung in Dashboards
- Dynamische Dashboards

Die Studierenden sollten auch mit den Inhalten der folgenden weiterführenden Kurse vertraut sein:

- Advanced Dashboards & Visualizations
- Splunk Enterprise System Administration (recommended)

Empfohlene Kenntnisse:

- Erfahrung mit HTML, CSS und XML/Erfahrung mit JavaScript
- Umgang mit einem Terminal-Texteditor (vi, Nano, etc.)

Kursziel

Splunk Certified Developer (Vorausgesetzt für diese Zertifizierung werden der Splunk Core Certified Power User UND Splunk Enterprise Certified Admin oder Splunk Cloud Certified Admin)

Stand 07.05.2025

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/SKDE

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 der Schweiz

4 Tage

Online Training

4 Tage CHF 3.855,-

Termin/Kursort

Kurssprache Deutsch

17.11.-20.11.25 Online



Inhaltsverzeichnis

Splunk - Developer Fast Start

Introduction to Dashboards :

Topic 1 - Dashboard Framework

Describe the dashboard definition
Compare classic and dashboard studio dashboards
Manage view
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 parameters
Apply dynamic coloring

Dynamic Dashboards :

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
Advanced Dashboards and Visualizations :

Module 1 – SplunkJS Dashboards

Identify view types
Create a SplunkJS dashboard
Define view properties, methods and events
List types of search managers

Module 2 – Using Tokens

Use tokens in SplunkJS
Define Splunk's token models
Describe how to get, set, and change tokens
Create a SplunkJS form

Module 3 – Using Event Handlers

Identify types of event handlers
Define event handler syntax
Define drilldown properties
Create an event handler

Module 4 – Creating Custom Visualizations

Define the custom visualization primary files
Add custom visualizations to views
Create a custom visualization
Define security best practices

Building Splunk Apps :

Module 1 – Planning App Development

Create a development environment
Improve app performance
Identify Splunk log files
Use security best practices
Create a data generator

Module 2 – Creating Apps

Define the web framework architecture
Identify ways to build Splunk apps
Manage apps and add-ons
Create an app
Configure app properties
Create app navigation

Module 3 – Adding Data

List types of data inputs
Identify ways to add data
Define when to use a scripted input
Create a modular input

Module 4 – Using the REST API

Explain how the Splunk REST API works
Define API endpoints
Explain how the KV Store works
Create a KV Store
Use lookups with a KV Store

Module 5 – Packaging Apps

Create an app setup screen
Define search time precedence
Explain local and default differences
Package an app
Developing with Splunk's REST API :

Module 1 – Introduction to the Splunk REST API

Introduce the Splunk development environment and its REST endpoints
Connect to the appropriate Splunk server 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
Identify 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
Use the rest command.

Module 3 – Parsing Output

Understand the general structure of Atom-based output
Format Atom-based XML and JSON output
Write code that uses the API and parse responses

Module 4 – Oneshot Searching

Review search language syntax and search best practices
Execute oneshot searches
Get search results and parse them

Module 5 – Normal and Export Searching

Identify types of searches
Execute normal and export searches
Get search results, job status and search job properties.

Module 6 – Advanced Searching and Job Management

Execute real-time searches
Work with large result sets
Work with saved searches
Manage search jobs

Module 7 – Working with Indexes

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

Appendix – Useful Admin REST APIs

Get system information
Manage Splunk configuration files
Manage Indexes

