

# Splunk - Developer Fast Start

**Introduction to Dashboards:** designed for power users who want to learn best practices for building and editing JSON-based dashboards in Dashboard Studio. It focuses on creating inputs, editing dashboard source code, chain searches, event annotations, and improving dashboard performance

**Dynamic Dashboards:** designed for power users who want to learn best practices for creating JSON-based, interactive dashboards in Dashboard Studio. It focuses on creating user inputs, editing dashboard source code, chain searches, event annotations, and improving dashboard performance.

**Advanced Dashboards and Visualizations:** designed for advanced users who want to create SplunkJS-based dashboards and forms. It focuses on creating dashboards, adding inputs, using event handlers and creating Splunk Custom Visualizations.

**Building Splunk Apps:** focuses on Splunk Enterprise app development. It's designed for advanced users, administrators, and developers who want to create apps using the Splunk Web Framework. Major topics include planning app development, creating data generators and data inputs; the REST API, setup screens, KV Store, and app packaging.

**Developing with Splunk's REST API:** for developers who want to use the Splunk REST API to interact with Splunk servers. In this course, use curl and Python to send requests to Splunk REST endpoints and learn how to parse and use the results. Create a variety of objects in Splunk, learn how to change properties, work with and apply security to Splunk objects, run different types of searches and parse its results, ingest data using the HTTP Event Collector and manipulate collections and KV Stores.

#### Kursinhalt

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

#### Voraussetzungen

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

- What is Splunk?
- Intro to Splunk
- Using Fields
- Visualizations
- Leveraging Lookups & Subsearches
- Correlation Analysis
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Introduction to Dashboards
- Dynamic Dashboards

Students should also understand the following advanced coursework:

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

Recommended Skills:

- Experience with HTML, CSS, and XML
- Experience with JavaScript
- Using a terminal text editor (vi, Nano, etc.)

#### Kursziel

Splunk Certified Developer (Prereq for this cert is the Splunk Core Certified Power User AND Splunk Enterprise Certified Admin OR Splunk Cloud Certified Admin)

#### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.de/go/SKDE](http://www.experteach.de/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.
<b>Termine in Deutschland</b>	<b>4 Tage € 3.500,-</b>
<b>Online Training</b>	<b>4 Tage € 3.500,-</b>
Termine auf Anfrage	

Stand 17.03.2024



# 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

desiredtask

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

