

Using the Splunk REST API (DSRAPI)

ID DSRAPI Preis auf Anfrage Dauer 9 Stunden

Zielgruppe

Dieser 9-stündige Kurs richtet sich an Entwickler, die die Splunk REST API zur Interaktion mit Splunk-Servern nutzen möchten.

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.

Voraussetzungen

Um erfolgreich zu sein, sollten die Studierenden über ein solides Verständnis der folgen:

- Splunk Grundlagen 1 und 2 (nicht mehr verfügbar)

Oder die folgenden Ein-Themen-Kurse:

- [Intro to Splunk \(ITS\)](#)
- [Using Fields \(Free\) \(SUFF\)](#) oder [Using Fields \(SUF\)](#)
- [Working with Time \(WWT\)](#)
- [Statistical Processing \(SSP\)](#)
- [Search Under the Hood \(SUH\)](#)
- [Intro to Knowledge Objects \(IKO\)](#)

Die Teilnehmer sollten auch die folgenden Kurse verstehen:

- [Splunk Enterprise Data Administration \(SEDA\)](#) (empfohlen)

Kursziele

- Einführung in die Splunk REST API
- Namespaces und Objektverwaltung
- Parsing-Ausgabe
- Oneshot-Suche
- Normale und Export-Suche
- Erweiterte Suche und Stellenverwaltung
- Zusammenarbeit mit KV Stores
- Verwendung des HTTP-Ereignissammlers (HEC)

Kursinhalt

In diesem Kurs verwenden Sie curl und Python, um Anfragen an Splunk REST-Endpunkte zu senden und lernen, wie Sie die Ergebnisse auswerten und verwenden. Erstellen Sie eine Vielzahl

Using the Splunk REST API (DSRAPI)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>