

Splunk Enterprise Data Administration (SEDA)

ID SEDA Preis auf Anfrage Dauer 18 Stunden

Zielgruppe

Dieses 13,5-stündige Modul richtet sich an Administratoren, die für die Einspeisung von Daten in Splunk Indexern verantwortlich sind.

Empfohlenes Training für die Zertifizierung zum

Splunk Enterprise Certified Admin (SECA)

Voraussetzungen

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

- Grundlagen 1 (nicht mehr verfügbar)
- Grundlagen 2 (empfohlen) (nicht mehr verfügbar)

Oder die folgenden Ein-Fach-Module:

- [Intro to Splunk \(ITS\)](#)
- [Using Fields \(SUF\)](#)
- [Intro to Knowledge Objects \(IKO\)](#)
- [Creating Knowledge Objects \(CKO\)](#)
- [Creating Field Extractions \(CFE\)](#)

Die Studierenden sollten auch das folgende Modul verstehen:

- !Splunk Enterprise System Administration (SESA) (empfohlen)

Kursziele

- Sourcetypen verstehen
- Verwalten und Bereitstellen von Forwardern
- Dateneingänge konfigurieren
- Datei-Monitore
- Netzwerkeingänge (TCP/UDP)
- Geskriptete Eingaben
- HTTP-Eingaben (über den HTTP Event Collector)
- Anpassen des Parsing-Prozesses der Eingabephase
- Definieren Sie Transformationen, um Daten vor der Indizierung zu ändern
- Konfigurationen von Wissensobjekten für die Suchzeit definieren

Kursinhalt

Das Modul vermittelt das grundlegende Wissen über Splunk-Forwarder und Methoden, um Remote-Daten in Splunk-Indexer zu bekommen. Es behandelt die Installation, Konfiguration, Verwaltung, Überwachung und Fehlerbehebung von Splunk-Forwardern und Splunk Deployment Server-Komponenten.

Splunk Enterprise Data Administration (SEDA)

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>