Splunk Enterprise Data Administration

This 13.5-hour course is designed for administrators who are responsible for getting data into Splunk Indexers. The course provides the fundamental knowledge of Splunk forwarders and methods to get remote data into Splunk indexers. It covers installation, configuration, management, monitoring, and troubleshooting of Splunk forwarders and Splunk Deployment Server components.

Course Topics

- Understand sourcetypes
- Manage and deploy forwarders
- Configure data inputs
- File monitors
- Network inputs (TCP/UDP)
- Scripted inputs
- HTTP inputs (via the HTTP Event Collector)
- Customize the input phase parsing process
- Define transformations to modify data before indexing
- Define search time knowledge object configurations

Prerequisite Knowledge

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

- Fundamentals 1
- Fundamentals 2 (recommended)

Or the following single-subject courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions

Students should also understand the following courses:

- Splunk Enterprise System Administration (recommended)

Course Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Course Objectives

Module 1 – Getting Data Into Splunk

- Provide an overview of Splunk
- Describe the four phases of the distributed model
- Describe data input types and metadata settings
- Configure initial input testing with Splunk Web
- Testing Indexes with Input Staging

Module 2 – Configuration Files

- Identify Splunk configuration files and directories
- Describe index-time and search-time precedence
- Validate and update configuration files

Module 3 – Forwarder Configuration

- Identify the role of production indexers and forwarders
- Understand and configure Universal Forwarders
- Understand and configure Heavy Forwarders
- Understand and configure intermediate forwarders
- Identify additional forwarder options

Module 4 – Forwarder Management

- Describe Splunk Deployment Server (DS)
- Manage forwarders using deployment apps
- Configure deployment clients and client groups
- Monitor forwarder management activities

Module 5 – Monitor Inputs

- Create file and directory monitor inputs
- Use optional settings for monitor inputs
- Deploy a remote monitor input

Module 6 – Network Inputs

- Create network (TCP and UDP) inputs
- Describe optional settings for network inputs

Module 7 – Scripted Inputs

- Create a basic scripted input

Module 8 – Agentless Inputs

- Configure Splunk HTTP Event Collector (HEC) agentless input
- Describe Splunk App for Stream

Module 9 – Operating System Inputs

- Identify Linux-specific inputs
- Identify Windows-specific inputs

Module 10 – Fine-tuning Inputs

- Understand the default processing that occurs during input phase
- Configure input phase options, such as source type fine-tuning and character set encoding

Module 11 – Parsing Phase and Data Preview

- Understand the default processing that occurs during parsing
- Optimize and configure event line breaking
- Explain how timestamps and time zones are extracted or assigned to events
- Use Data Preview to validate event creation during parsing phase

Module 12 – Manipulating Raw Data

- Explain how data transformations are defined and invoked
- Use transformations with props.conf and transforms.conf to:
  - Mask or delete raw data as it is being indexed
  - Override sourcetype or host based upon event values
  - Route events to specific indexes based on event content
  - Prevent unwanted events from being indexed
- Use SEDCMD to modify raw data

Module 13 – Supporting Knowledge Objects

- Define default and custom search time field extractions
- Identify the pros and cons of indexed time field extractions
- Configure indexed field extractions
- Describe default search time extractions
- Manage orphaned knowledge objects

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/education

To contact us, email Education_AMER@splunk.com

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

Contact sales