splunk>

Splunk Enterprise Data Administration

This 3 virtual day 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

- Deploy forwarders with Forwarder Management
- Splunk Configuration Files
- Configure common Splunk data inputs
- Customize the input parsing process

Course Prerequisites

- Required:
- Splunk Fundamentals 1
- Splunk Fundamentals 2
  - Strongly Recommended:
- Splunk Enterprise System Administration

Class Format

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

Course Modules

Module 1 – Introducing Splunk Data Administration

- Provide an overview of Splunk
- Describe the four phases of the distributed model
- Identify Splunk configuration files and directories
- Describe index-time and search-time precedence
- Use btool to retrieve configuration information

Module 2 – Getting Data In – Staging

- List the four phases of Splunk Indexing
- Describe data input types and default metadata settings
- Describe differences between the input and parsing phase
- Configure initial input testing with Splunk Web

Module 3 – Forwarder Configuration

- Understand the role of production indexers and forwarders
- Understand the functionality of Universal Forwarders
- Configure forwarders
- Identify additional forwarder options

Module 4 – Heavy Forwarders & Forwarder Management

- Describe what the heavy forwarder is and use cases
- Perform heavy forwarder configuration
- Deploy an app to the heavy forwarder
- 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 and Scripted Inputs

- Create network (TCP and UDP) inputs
- Describe optional settings for network inputs
- Create a basic scripted input

Module 7 – Windows and Agentless Inputs

- Identify Windows specific inputs.conf stanzas and attributes
- Understand and configure Splunk HTTP Event Collector (HEC) agentless input
- Monitor HEC using MC (Monitoring Console)

Module 8 – Fine-tuning Inputs

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

Module 9 – 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 the parsing phase

Module 10 – 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 11 – Supporting Knowledge Objects

- Define default and custom search time field extractions
- Define the pros and cons of index time field extractions
- Configure indexed field time 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 of Splunk Education's course offerings, or to register for a course, go to https://www.splunk.com/en_us/training/faq-training.html

- To contact us, email education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
250 Brannan
San Francisco, CA
94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com