

Splunk Enterprise Data Administration

(SP-SEDA)



COURSE OVERVIEW

This 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.



PREREQUISITES

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- Intro to Splunk (ITS)
- Using Fields (SUF)
- Intro to Knowledge Objects (IKO)
- Creating Knowledge Objects (CKO)
- Creating Field Extractions (CFE)
- Enriching Data with Lookups (EDL)
- Data Models (SDM)

Additional courses and/or knowledge in these areas are also highly recommended:

- Troubleshooting Splunk Enterprise (TSE)
- Splunk Enterprise Cluster Administration (SCLA)
- Transitioning to Splunk Cloud (TSC)



COURSE OUTLINE

Module 1 - Get 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



Splunk Enterprise Data Administration

(SP-SEDA)



COURSE OUTLINE

Module 2 - Configuration Files and Apps

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

Module 3 - Configure Forwarders

- Configure Universal Forwarders
- Configure Heavy Forwarders

Module 4 - Customize Forwarder

- Configure intermediate forwarders
- Identify additional forwarder options

Module 5 - Manage Forwarders

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

Module 6 - Monitor Inputs

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

Module 7 - Network Inputs

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

Module 8 - Scripted Inputs

- Create a basic scripted input

Module 9 - Agentless Inputs

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



Splunk Enterprise Data Administration

(SP-SEDA)



COURSE OUTLINE

Module 10 - Operating System Inputs

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

Module 11 - 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 12 - 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 13 - Manipulating Input Data

- Explore Splunk transformation methods
- Create rulesets with Ingest Actions
- Mask data with Ingest Actions rules
- Mask data with SEDCMD and TRANSFORMS

Module 14 - Routing Input Data

- Filter data with Ingest Action rules
- Route data with Ingest Action rules
- Route data with Transforms

Module 15 - 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

