Splunk Enterprise Data Administration

Course Description:

This course is 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 Duration:

2 Days

Prerequisites:

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

- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Splunk Enterprise System Administration

Course Outlines:

Module 1 – Get Data into Splunk

- Provide an overview of Splunk
- Describe the Splunk distributed model
- Describe data input types and metadata settings
- Configure initial input testing with Splunk Web
- Test indexes with input staging

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 app installation

Module 3 – Configure Forwarders

- Configure universal forwarders
- Configure heavy forwarders

Module 4 – Customize Forwarders

- Configure intermediate forwarders
- Identify additional forwarder options

Module 5 – Manage Forwarders

- Describe the Splunk deployment server
- 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

Module 10 – Operating System Inputs

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

Module 11 – Fine-tune Inputs

- Understand the default processing that occurs during input phase
- Configure input phase options

Module 12 – Parsing Phase and Data Preview

- Understand default processing during parsing phase
- Optimize and configure event line breaking
- Explain how timestamps and time zone are used
- Use Data Preview to validate event create during parsing phase

Module 13 – Manipulate Input Data

- Explore Splunk transformation methods
- Create rulesets with Ingest Actions
- Mask data with Ingest Action rules
- Mask data with SEDCMD and TRANSFORMS
- Override sourcetype or host based upon event values

Module 14 – Route Input Data

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

Module 15 – Support 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

Target Audience:

- Administrators