SPLUNK EDUCATION

Course Description

Splunk Enterprise Data Administration

Summary

This course is for administrators who are responsible for getting data into Splunk.

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 Agent Management Server components.

Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
  - Exploring Splunk Platform Ecosystem
  - Splunk User Track
  - Splunk Enterprise System Administration

Format: Instructor-led

Duration: 18 hours

Audience: Administrators

Course Outline

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 Agents

- Explain the features and benefits of agent management
- List the agent management components
- Configure agents
- Create deployment apps
- Deploy apps to agents using server classes created in agent management
- Monitor forwarder activity using the Monitoring Console
- Monitor agent 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
- Describe the process for creating and deploying scripted inputs
- Identify the potential risks associated with scripted inputs

Module 9 – Agentless Inputs

- Configure Splunk HTTP Event Collector (HEC)
- Describe HEC deployment options
- Explain how HEC indexer acknowledgement works
- Monitor HEC activity using the MC
- Examine Splunk Edge Hub
- 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 – Parse Phase and Data Preview

- Understand the default processing that occurs during parsing
- Optimize and configure event line breaking
- Explain how timestamps and time zone are extracted/assigned to events
- Use Data Preview to validate event creation during the 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 source type or host based upon event values

Module 14 – Route Input Data

- Route and filter events using classic TRANSFORMS methods
- Use TRANSFORMS and forwarding groups to send events from heavy forwards to specific groups of indexers
- Use Ingest Actions to conditionally route and filter events

Module 15 – Support Knowledge Objects

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

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit http://www.splunk.com/education.

To contact us, email education@splunk.com.