Splunk Enterprise Data Administration (SEDA)

Course ID #: 7000-1110-ZZ-Z
Hours: 21

Course Content

Description:

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.

Objectives:

Upon successful completion of this course, students will:

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
Intro to Splunk, Using Fields (SUF), Intro to Knowledge Objects, Creating Knowledge Objects (CKO), Creating Field Extractions (CFE), Enriching Data with Lookups (EDL), Data Models (SDM), and Splunk Enterprise System Administration (SESA)

Target Audience:

Administrators

Topics:

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 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 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

Splunk Enterprise Data Administration (SEDA)

Course ID #: 7000-1110-ZZ-Z

Hours: 21

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

Module 12 – Parsing Phase and Data Preview
- Understand the default processing during parsing phase
- Optimize and configure event line breaking
- Explain how timestamps and time zones are used
- Use Data Preview to validate event create 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
- Override sourcetype or host base upon event values

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

Register for this class by visiting us at:
www.tcworkshop.com or by calling us at 800-639-3535

NASBA CPE details are provided on the following pages.

Splunk Enterprise Data Administration (SEDA)

Course ID #: 7000-1110-ZZ-Z
Hours: 21

NASBA Information

Level:
Advanced Preparation:
Attendance Requirement: To be awarded the full credit hours, you must sign in and attend the entire course.
Recommended Field(s) of Study:
Recommended CPEs: 23.40

Policies: Course Registration, Cancellation, Refund, and Complaint Resolution
For more information regarding administrative policies such as complaint and program cancellation policies, please contact our offices at 800-639-3535 or visit us at: **www.tcworkshop.com**

Official National Registry Statement:
The Computer Workshop is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

NOTE: Since our information is in multiple places on our website or in PDF format that is sent to clients, we have provided our normal course content with the NASBA Information added along with links to our policy page on the web. We will add our name to the Official National Registry Statement after we are approved.