Splunk Enterprise System Administration (SESA)

Course ID #: 7000-1109-ZZ-Z
Hours: 14

Course Content

Description:

This course is designed for system administrators who are responsible for managing the Splunk Enterprise environment. The course provides the fundamental knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components

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), and Data Models (SDM)

Target Audience:

Administrators

Modules:

Module 1 - Deploy Splunk

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- List the steps to install Splunk
- Use Splunk CLI commands
- Explore security best practices

Module 2 - Monitor Splunk

- Use Splunk Health Report
- Enable the Monitoring Console (MC)
- Use Splunk Assist
- Use Splunk Diag

Module 3 - License Splunk

- Identify Splunk license types
- Describe license violations
- Add and remove licenses

Module 4 - Use Configuration Files

- Describe Splunk configuration directory structure
- Understand configuration layering process
- Use btool to examine configuration settings

Module 5 - Use Apps

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

Module 6 - Create Indexes

- Learn how Splunk indexes functions
- Identify the types of index buckets
- Add and work with indexes
- Overview of metrics index

Module 7 - Manage Index

- Review Splunk Index Management basics
- Identify data retention recommendations
- Identify backup recommendations
- Move and delete index data
- Describe the use of the Fishbucket
- Restore a frozen bucket

Module 8 - Manage Users

- Add Splunk users using native authentication
- Describe user roles in Splunk
- Create a custom role
- Manage users in Splunk

Module 9 - Configure Basic Forwarding

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the Deployment Server

Module 10 - Configure Distributed Search

- Describe how distributed search works
- Describe the roles of the search head and search peers

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 System Administration (SESA)

Course ID #: 7000-1109-ZZ-Z
Hours: 14

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: 15.60

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.