Troubleshooting Splunk Enterprise (SP-TSE)

COURSE OVERVIEW

This 9-hour course is designed for Splunk administrators. It covers topics and techniques for troubleshooting a standard Splunk distributed deployment using the tools available with Splunk Enterprise.

This lab-oriented class is designed to help you gain troubleshooting experience before attending more advanced courses. You will debug a distributed Splunk Enterprise environment using the live system.

This course does not cover the issues surrounding Splunk Cloud, Splunk Clusters, or Splunk premium apps.

PREREQUISITES

To be successful, students should have a solid understanding of the following modules:

- Splunk Fundamentals 1 (Retired)
- Splunk Fundamentals 2 (Retired)

Or the following single-subject modules:

- What is Splunk? (Retired)
- Intro to Splunk (ITS)
- Search Under the Hood (SUH)
- Scheduling Reports & Alerts (SRA)
- Visualizations (SVZ)
- Leveraging Lookups and Subsearches (LLS)
- Search Under the Hood (SUH)
- Intro to Knowledge Objects (IKO)
- Creating Knowledge Objects (CKO)
- Creating Field Extractions (CFE)
- Enriching Data with Lookups (EDL)
- Data Models (SDM)

Student should also have completed the following modules:

- Splunk Enterprise System Administration (SESA)
- Splunk Enterprise Data Administration (SEDA)
- Course Objectives
- Splunk Troubleshooting Methods and Tools
- Indexing Problems
- Input Configuration Problems
- Deployment Problems
- License, Upgrade, and User Management Problems
- Search Management Problems
- User Search Problems

WHO SHOULD ATTEND

Splunk administrators.

Troubleshooting Splunk Enterprise (SP-TSE)

COURSE OUTLINE

Module 1 – Splunk Troubleshooting Methods and Tools

- Describe the Splunk Troubleshooting Approach
- List Splunk Diagnostic Resources and Tools
- Create and Splunk a Diag
- Use RapidDiag

Module 2 – Indexing Problems

- Discover Splunk Deployment Topology and its Server Roles
- Identify Where to Check the Index-Time Pipeline Status
- Use the metrics.log to Clarify the Index-Time Problem

Module 3 – Input Configuration Problems

- Data Input Issues
- Troubleshooting Inputs with the Monitoring Console

Module 4 – Input Configuration Problems

- Deployment Server Issues
- Forwarding and Receiving Issues

Module 4 – Indexer Cluster Management Administration

- Peer Offline and Decommission
- Master App Bundles
- Indexer Cluster Storage Utilization Options
- Site Mapping
- Monitoring Console for Indexer Cluster Environment

Module 5 – License, Upgrade, and User Management Problems

- Installation Issues
- Upgrade Considerations
- Splunk Licensing Issues
- Splunk Roles and User Management Issues

Module 6 – Search Head Management Problems

- Troubleshoot Distributed Search Issues
- Identify Job Scheduling Problems
- Learn to Diagnose Crashing Problems
- Describe How to Prioritize Resources for Critical Splunk Processes

Module 7 – KV Store Collection and Lookup Management

- Identify the Types of Search Problems
- Isolate and Troubleshoot Search Problems