# Troubleshooting Splunk Enterprise

## Course Description:

This course is for Splunk administrators.

The course covers topics and techniques for troubleshooting a standard Splunk distributed deployment using the tools available with Splunk Enterprise.

## 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
- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

Additional courses and/or knowledge in these areas are also highly recommended:

- Enriching Data with Lookups
- Data Models

## Course Outlines:

### 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 – Deployment and Forwarder Problems

- Deployment Server Issues
- Forwarding and Receiving Issues

### Module 5 – Search 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 6 – User Search Problems

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

## Target Audience:

- Administrators