Troubleshooting Splunk Enterprise

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.

Course Topics

- Splunk Troubleshooting Methods and Tools
- Indexing Problems
- Input Configuration Problems
- Deployment Problems
- License, Upgrade, and User Management Problems
- Search Management Problems
- User Search Problems

Prerequisite Knowledge

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

- Splunk Fundamentals 1
- Splunk Fundamentals 2

Or the following single-subject courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Leveraging Lookups and Sub-searches
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards

Student should also have completed the following courses:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

Course Format

Instructor-led lecture with labs, delivered via virtual classroom or at your site.

Course Objectives

- Understand the Splunk Support Model and its resources
- Identify the best practices for troubleshooting Splunk Enterprise
- List ways to gather useful Splunk diagnostic information
- Use Splunk diagnostic tools
- Identify common Splunk technical issues and solve them

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

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/education

To contact us, email Education_AMER@splunk.com

Splunk, Inc.
270 Brannan St. San Francisco, CA 94107
+1 866.GET.SPLUNK (1 866.438.7758)
Contact sales