

Troubleshooting Splunk Enterprise 8.2

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 Monitoring Console

Module 4 – Deployment Problems

- Deployment server issues
- Forwarding and receiving issues

Module 5 – License, Upgrade, and User Management Problems

- Installation issues
- Upgrade considerations
- Splunk licensing issues
- Splunk roles and user management issues

Module 6 – Search Management Problems

- Troubleshoot distributed search issues
- Identify job scheduling issues
- Learn to diagnose crashing problems
- Describe how to prioritize resources for critical Splunk processes

Module 7 – User Search Problems

- Identify the types of search problems
- Isolate and troubleshoot search problems