

Search Optimization

Course Description:

This course is for power users who want to improve search performance.

The course will cover how search modes affect performance, how to create an efficient basic search, how to accelerate reports and data models, and how to use the `tstats` command to quickly query data.

Course Duration:

1 Day

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- How Splunk works
- Creating search queries
- Creating reports and data models

Course Outlines:

Module 1 – Optimize Search

- Understand how search modes affect performance
- Examine the role of the Splunk Search Scheduler
- Review general search practices

Module 2 – Report Acceleration

- Define acceleration and acceleration types
- Understand report acceleration and create an accelerated report
- Reveal when and how report acceleration summaries are created
- Search against acceleration summaries

Module 3 – Data Model Acceleration

- Understand data model acceleration
- Accelerate a data model
- Use the `datamodel` command to search data models

Module 4 – Using the `tstats` Command

- Explore the `tstats` command
- Search acceleration summaries with `tstats`
- Search data models with `tstats`
- Compare `tstats` and `stats`

Target Audience:

- Knowledge Managers
- Users/Analysts