Intro to Splunk

This eLearning course teaches students how to use Splunk to create reports and dashboards and explore events using Splunk's Search Processing Language. Students will learn the basics of Splunk's architecture, user roles, and how to navigate the Splunk Web interface to create robust searches, reports, visualizations, and dashboards..

Course Topics

- Introduction to Splunk's interface
- Basic searching
- Using fields in searches
- Search fundamentals
- Transforming commands
- Creating visualizations
- Creating reports and dashboards
- Identifying types of knowledge objects

Prerequisite Knowledge

None

Course Format

eLearning

Course Objectives

Topic 1 – Intro to Splunk

- Splunk components
- Basic Splunk functions

Topic 2 – Using Splunk

- Define Splunk apps
- Understand Splunk user roles
- Search & Reporting app
- Splunk Web interface

Topic 3 – Using Search

- Run basic searches
- Set the time range of a search
- Save search results
- Identify the contents of search results
- Work with events
- Share search jobs
- Export search results
- Select search modes
- Control a search job

Topic 4 - Exploring Events

- Refine searches
- Understand timestamps
- Use the events tab to add and remove terms from a search

Topic 5 – Search Processing Language

- Use wildcards to search for multiple terms
- Understand case sensitivity in searches
- Use booleans to include and exclude search criteria
- Use special characters with search terms

Topic 6 – What are Commands?

- Understand the anatomy of Splunk's search language:
  - Search terms
  - Commands
  - Functions
  - Arguments
  - Clauses
- Understand best practices for writing searches

Topic 7 – What are Knowledge Objects?

- Identify the five categories of knowledge objects:
  - Data interpretation
  - Data classification
  - Data Enrichment
  - Data Normalization
  - Data Models
- Understand types of knowledge objects

Topic 8 – Creating Reports and Dashboards

- Save a search as a report
- Edit reports
- Use transforming commands to create visualizations
- Create a dashboard
- Add a report to a dashboard
- Edit a dashboard

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

Using Fields

This three-hour course is for power users who want to learn about fields and how to use fields in searches. Topics will focus on explaining the role of fields in searches, field discovery, using fields in searches, and the difference between persistent and temporary fields. The last topic will introduce how fields from other data sources can be used to enrich search results.

Course Topics

- What are Fields?
- What is Field Discovery?
- Use Fields in Searches
- Compare Temporary versus Persistent Fields
- Enrich Data

Prerequisite Knowledge

To be successful, students should have completed the following courses:

- Search Under the Hood
- Multivalue Fields
- Creating Knowledge Objects

Course Format

Instructor-led or eLearning

Course Objectives

Topic 1 – What are Fields?

- Define fields and field auto-extraction
- Explore the Fields sidebar
- Add fields to the Selected Fields list
- Explore and generate reports from the Fields window

Topic 2 – What is Field Discovery?

- Understand Field Discovery
- Explore search modes and their effect on search results

Topic 3 – Use Fields in Searches

- Use fields correctly in basic searches
- Use fields with operators
- Use the rename command
- Use the fields command to improve search performance

Topic 4 – Compare Temporary versus Persistent Fields

- Differentiate between temporary and persistent fields
- Create temporary fields with the eval command
- Extract temporary fields with the erex and rex commands

Topic 5 – Enrich Data

- Understand how fields from lookups, calculated fields, field aliases, and field extractions enrich data

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

Scheduling Reports & Alerts

This eLearning course teaches students how to use scheduled reports and alerts to automate processes in their organization. Students will create, manage, and schedule reports and alerts, and use alert actions to further respond to incidents as they occur.

Course Topics

- Creating and managing Scheduled Reports
- Creating and managing Alerts
- Using Alert Actions

Prerequisite Knowledge

Recommended:

Intro to Splunk eLearning course

Intro to Knowledge Objects eLearning course

Required:

none

Course Format

eLearning

Course Objectives

Topic 1 – Creating a Scheduled Report

- Create a report
- Schedule a report
- Define a report's time range
- Define schedule priority
- Define schedule window
- Add a trigger condition

Topic 2 – Managing Reports

- View report settings
- Edit report permissions
- Enable report embedding

Topic 3 – Creating Alerts

- Save a search as an alert
- Define alert permissions
- Understand scheduled and real-time alert types
- Define alert trigger conditions

Topic 4 – Using Alert Actions

- Define actions that respond to trigger conditions
- Write results to a log event
- Output results to a lookup
- Output results to a telemetry endpoint
- Send an email containing search results
- Set up a webhook alert action

Topic 5 – Managing Alerts

- View alert settings
- Edit alert permissions

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

Visualizations

This eLearning course teaches students how to create visualizations in Splunk, using Splunk's Search Processing Language as well as the Splunk Web interface. Students will learn commands that allow data to be displayed on charts and graphs, transform geographic data into maps, create single value visualizations, and use Splunk's visual formatting options to change the look of statistical tables.

Course Topics

- Formatting data using transforming commands
- Preparing data for use in visualizations
- Generating maps using geographic data
- Creating and customizing single value visualizations
- Visually formatting statistical tables

Prerequisite Knowledge

Recommended:

Intro to Splunk eLearning course

Required:

none

Course Format

eLearning

Course Objectives

Topic 1 – Formatting Commands

- The fields command
- The table command
- The dedup command
- The addtotals command
- The fieldformat command

Topic 2 – Visualizing Data

- Explore visualization types
- Use transforming commands to order results into a data table:
  - top
  - rare
  - stats
  - chart
  - timechart
  - trendline
- Understand when to use different transforming commands

Topic 3 – Generating Maps

- Explore geographic visualization types
- Use commands specific to geographic data
  - iplocation
  - geostats
  - geom
- Prepare data for use in a choropleth map

Topic 4 – Single Value Visualizations

- Use visual formatting options for single value visualizations
- Add a sparkline to a single value visualization
- Use the Trellis layout to split visualizations
- Use the gauge command
- Use the radial, filler, and marker gauge visualization types

Topic 5 – Visual Formatting

- Explore formatting options for statistical tables
- Create a chart overlay
- Explore formatting options for different types of visualizations

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

Working with Time

This three-hour course is for power users who want to become experts at using time in searches. Topics will focus on searching and formatting time in addition to using time commands and working with time zones.

Course Topics

- Searching with Time
- Formatting Time
- Comparing Index Time versus Search Time
- Using Time Commands
- Working with Time Zones

Prerequisite Knowledge

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

- How Splunk works
- Creating search queries
- The eval command

Course Format

Instructor-led or eLearning

Course Objectives

Topic 1 – Searching with Time

- Understand the _time field and timestamps
- View and interact with the Event Timeline
- Use the earliest and latest time modifiers
- Use the bin command with the _time field

Topic 2 – Formatting Time

- Use various date and time eval functions to format time

Topic 3 – Using Time Commands

- Use the timechart command
- Use the timewrap command

Topic 4 – Working with Time Zones

- Understand how time and timezones are represented in your data
- Determine the time zone of your server
- Use strftime to correct timezones in results

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

Statistical Processing

This four-hour course is for power users who want to identify and use transforming commands and eval functions to calculate statistics on their data. Topics will cover data series types, primary transforming commands, mathematical and statistical eval functions, using eval as a function, and the rename and sort commands.

Course Topics

- What is a Data Series
- Transforming Data
- Statistical Aggregation with the stats Command
- Manipulating Data with eval
- Formatting Data

Required (Prerequisite) Knowledge

To be successful, students should have a working understanding of these courses:

- What is Splunk?
- Intro to Splunk
- Using Fields

Recommended Knowledge

To be successful, students are recommended (but not required) to have a working understanding of these courses:

- Visualizations
- Result Modification

Course Format

Instructor-led or eLearning

Course Objectives

Topic 1 – What is a Data Series

- Introduce data series
- Explore the difference between single-series, multi-series, and time series data series

Topic 2 – Transforming Data

- Use the chart, timechart, top, and rare commands to transform events into data tables

Topic 3 – Statistical Aggregation with the stats Command

- Define aggregation
- Explore the stats command and eight of its functions

Topic 3 – Manipulating Data with eval Command

- Explore the eval command
- Explore and perform calculations using mathematical and statistical eval functions
- Perform calculations and concatenations on field values
- Use the eval command as a function with the stats command

Topic 4 – Formatting Data

- Use the rename command
- Use the sort command

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

Leveraging Lookups and Subsearches

This three-hour course is designed for power users who want to learn how to use lookups and subsearches to enrich their results. Topics will focus on lookup commands and explore how to use subsearches to correlate and filter data from multiple sources.

Course Topics

- Using Lookup Commands
- Adding a Subsearch
- Using the return Command

Required (Prerequisite) Knowledge

To be successful, students should have a working understanding of these courses:

- What is Splunk?
- Intro to Splunk
- Intro to Knowledge Objects
- Using Fields

Recommended Knowledge

To be successful, students are recommended (but not required) to have a working understanding of these courses:

- Creating Knowledge Objects

Course Format

Instructor-led or eLearning

Course Objectives

Topic 1 – Using Lookup Commands

- Understand lookups
- Use the inputlookup command to search lookup files
- Use the lookup command to invoke field value lookups
- Use the outputlookup command to create lookups
- Invoke geospatial lookups in search

Topic 2 – Adding a Subsearch

- Define subsearch
- Use subsearch to filter results
- Identify when to use subsearch
- Understand subsearch limitations and alternatives

Topic 3 – Using the return Command

- Use the return command to pass values from a subsearch
- Compare the return and fields commands

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

Intro to Knowledge Objects

This eLearning course teaches students about how different types of knowledge objects to extract additional insights from your data. Students will learn the basics of how to create knowledge objects, define their settings, edit, and manage existing knowledge objects.

Course Topics

- Using knowledge objects to discover and analyze data
- Developing naming conventions for knowledge objects
- Defining permissions for knowledge objects
- Managing knowledge objects

Prerequisite Knowledge

Recommended:

Intro to Splunk eLearning course

Required:

none

Course Format

eLearning

Course Objectives

Topic 1 – What are Knowledge Objects?

- Understand the different types of knowledge objects:
  - Fields
  - Field extractions
  - Field aliases
  - Calculated fields
  - Lookups
  - Event types
  - Tags
  - Workflow actions
  - Reports
  - Alerts
  - Macros
  - Data models

Topic 2 – Knowledge Object Settings

- Define naming conventions
- Define role-based permissions for knowledge objects

Topic 3 – Managing Knowledge Objects

- Edit knowledge objects
- Reassign knowledge objects

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

Search Optimization

This three-hour course is for power users who want to improve search performance. Topics 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 Topics

- Optimize Search
- Report Acceleration
- Data Model Acceleration
- Using the tstats Command

Prerequisite Knowledge

To be successful, students should have completed the following prerequisite courses:

- Search Under the Hood
- Multivalue Fields
- Scheduling Reports & Alerts
- Data Models

Course Format

Instructor-led or eLearning

Course Objectives

Topic 1 – Optimize Search

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

Topic 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

Topic 3 – Data Model Acceleration

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

Topic 4 – Using the tstats Command

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

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

Building Splunk Classic Apps

This 9-hour course focuses on Splunk app and add-on development. It's designed for application developers who want to create new apps for Splunk Enterprise and Splunk Cloud. Major topics include planning apps, building a data generator, creating custom search commands and REST endpoints, app packaging and deployment, and more.

Course Objectives

- Plan, build, and manage Splunk apps
- Create a data generator
- Develop a custom search command
- Extend the Splunk REST API
- Construct a workflow action
- Validate an app with AppInspect
- Package and deploy an app

Prerequisite Knowledge

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

- Splunk system administration
- Splunk data administration
- Python or a similar scripting language

Course Format

Instructor-led lecture with lab exercises. Delivered via virtual classroom or at your site.

Course Topics

Topic 1 – Planning Apps

- Describe apps and add-ons
- Set up a development environment
- Improve app performance
- Use security best practices

Topic 2 – Adding Data

- List types of data inputs
- Explain modular vs scripted inputs
- Review types of knowledge objects
- Create a data generator

Topic 3 – Creating Apps

- Create a basic app
- Configure app properties
- Identify app components
- Manage apps and add-ons

Topic 4 – Custom Search Commands

- Identify search command types
- Create a search command
- Examine Splunk metadata
- Configure access control

Topic 5 – Custom REST Endpoints

- Identify REST handler types
- Create a REST endpoint
- Examine Splunk metadata
- Configure access control

Topic 6 – Custom Workflow Actions

- Identify workflow action types
- Create a workflow action
- Examine workflow action parameters
- Configure access control

Topic 7 – Packaging Apps

- Create an app setup page
- Explain config file precedence
- Use AppInspect to validate an app
- Produce a deployable app

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