



Administrating Splunk

This six-hour course prepares system administrators to configure and manage a Splunk installation. It is recommended for administrators who will be in charge of ongoing management of Splunk servers.

Course Topics:

- Installing, stopping, starting and restarting Splunk
- Data Inputs and configuring data source
- How Splunk indexes data
- Setting up Splunk users
- Managing Splunk indexes
- Distributed search
- Data routing
- Deployment server

Course Prerequisites:

- The Using Splunk course
- Knowledge of UNIX directory and file commands
- Familiarity with networking concepts such as tcp, udp and ports

Class Format

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

Course Objectives

Lesson One - Installation and startup

- Splunk installation requirements and process
- List the steps needed to install on a non-standard location
- Stop and start Splunk
- Navigate through the Splunk directory tree

Lesson Two - Data Inputs

- Configure data sources using the Splunk web interface
- Configure data sources through the command line
- Determine which source type options to use
- Describe bundles and explain when they are used
- Define extracted fields and explain how they make searching and trouble shooting easier.

Lesson Three- Index Management

- Backup and restore an index
- Clean an index
- Control what is indexed

Lesson Four - Distributed Deployment

- Describe Splunk's distributed capabilities
- Describe the capabilities of the Splunk's deployment server
- Enable forwarding and receiving and distributed searches

Lesson Five - Defining Users

- List the Splunk roles and their capabilities
- Add and remove users
- Use ldap to configure users

Pricing

- Per student, \$1000
- Four - six users in the same class - \$3500
- Onsite education sessions require payment of instructor's travel and living expenses

Splunk Education Tracks

The Administrating Splunk class is one class in a full education program. The below chart shows how it combines with other classes for different types of users.

User: For all day-to-day Splunk users including customer support staff, developers, systems administrators and management.

Administrator: For administrators of Splunk itself. (Administrators of other systems who will just be using Splunk should take the User track.)

Architect: For architects who will be designing Splunk deployments, including architects on staff at customer deployments as well as partner professional services personnel.

Developer: For developers who will integrate, customize and extend Splunk using its APIs and advanced configuration bundling. (Developers of other applications who will just be using Splunk should follow the User track.)

Sales Engineer: For Splunk OEM and channel partner sales engineering staff who will be selling Splunk.

Support Engineer: For Splunk OEM and channel partner support staff who will be providing first line support for Splunk.

Tracks	Classes					
	Using Splunk	Administrating Splunk	Deploying Splunk	Developing with Splunk	Selling Splunk	Supporting Splunk
User	✓					
Administrator	✓	✓				
Architect	✓	✓	✓	✓		
Developer	✓	✓		✓		
Sales Engineer	✓	✓			✓	
Support Engineer	✓	✓				✓

About Splunk

Splunk is software that indexes, manages and enables you to search logs and IT data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
 118 King Street
 5th Floor
 San Francisco, CA 94107
 866.GET.SPLUNK
 (866.438.7758)
sales@splunk.com
support@splunk.com