



Deploying Splunk

This 1-day workshop focuses on designing a Splunk deployment. You will learn to assess your IT search requirements, design a Splunk topology, perform capacity planning and decide on indexing, security, and data management strategies.

Course Topics:

- Determining requirements
- Common deployment topologies
- What, how and where to index
- Data management policy
- Management and configuration of large deployments

Course Prerequisites:

- The Using Splunk course
- The Administrating Splunk course

Class Format

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

Course Description

Assess project objectives and gathering data

We begin by defining project goals. You will be guided through the process of information gathering by conducting a source, user, device and application inventory and producing an estimate of data volume for each data source. For user interviews, you will learn what questions to ask to determine user requirements and the data they require.

Design index strategy

Once you have identified data sources, consider how, what and where to index. You have choices on how Splunk processes and classifies data. You might wish to change default processing of timestamps, host names, and event boundaries or augment the default processing by defining meta events and defining additional fields.

Design a topology and conduct capacity planing

With your data inventory and index strategy you are now ready to plan where to place Splunk and where to index. As part of this process, you will also access your requirements for distributed processing, high availability, data segregation, and load balancing.

Design a data management policy

What are your requirements for retention and archiving? What about security and integrity - will you need to prove data has not been compromised? Do you need to control

who has access to specific data? Lean what options are available for these requirements.

Design a server management strategy

How will you manage your Splunk servers as you introduce new versions and new data sources and bundles? Do you have an in house configuration management tool you wish to use to manage Splunk or do you wish to use the Spunk Deployment server or use both?

Splunk Education Tracks

The Deploying Splunk class is one class in a full education program. See the chart below for a list of other classes.

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)