Splunk 6.2 Administration

This 20-hour course prepares system administrators to configure and manage Splunk. Topics include installation, data inputs and forwarder configuration, data management, user accounts, licenses, distributed search, and basic monitoring and troubleshooting. The focus in this class is the knowledge, best practices, and configuration details for Splunk administration in a small to medium distributed deployment environment.

Course Topics

- Installation
- License management
- Getting data in
- Managing Splunk apps
- Splunk configuration files
- Universal forwarder and forwarder management
- Data inputs in detail
- Index administration, maintenance and optimization
- Users, roles, and authentication
- Event Parsing with data preview
- Manipulating raw data
- Field extraction
- Distributed search
- Search performance tuning
- Introduction to large-scale Splunk deployment
- Monitoring and troubleshooting

Course Prerequisites

Required:

- Using Splunk
- Splunk Architecture Overview (eLearning)

Strongly Recommended:

- Searching and Reporting with Splunk
- Creating and Managing Splunk Knowledge Objects

Class Format

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

Course Modules

Building a Simple Splunk Environment

- Module 1 – Splunk Installation
- Module 2 – License Management
- Module 3 – Getting Data in
- Module 4 – Managing Apps

Building a Basic Production Environment

- Module 5 – Splunk Configuration Files
- Module 6 – Universal Forwarder
- Module 7 – Forwarder Management

Getting Data In

- Module 8 – Monitor Inputs
- Module 9 – Network Inputs
- Module 10 – Scripted and Modular Inputs
- Module 11 – Windows Inputs
- Module 12 – Fine-tuning Inputs

Managing Indexes and Users

- Module 13 – Splunk Indexes
- Module 14 – Index Maintenance and Optimization
- Module 15 – Users, Roles, and Authentication

Parsing

- Module 16 – Parsing Phase and Data Preview
- Module 17 – Manipulating Raw Data
- Module 18 – Field Extraction

Scaling Searches and Monitoring

- Module 19 – Distributed Search
- Module 20 – Search Performance Tuning
- Module 21 – Implementation issues in large-scale deployment
- Module 22 – Distributed Management Console

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 of Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/goto/education
To contact us, email Education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search 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.
250 Brannan
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com