Splunk Enterprise System Administration

This 2 virtual day course is designed for system administrators who are responsible for managing the Splunk Enterprise environment. The course provides the fundamental knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components.

Course Topics

- Splunk Deployment Overview
- License Management
- Splunk Apps
- Splunk Configuration Files
- Users, Roles, and Authentication
- Getting Data In
- Distributed Search

Course Prerequisites

Required:

- Splunk Fundamentals 1
- Splunk Fundamentals 2

Class Format

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

Course Modules

Module 1 – Splunk Deployment Overview

- Provide an overview of Splunk
- Identify Splunk components
- Identify Splunk system administrator role
- Identify Splunk installation steps
- Use Splunk CLI
- Enable the Monitoring Console (MC)

Module 2 – License Management

- Identify license types
- Describe license violations
- Add and remove licenses

Module 3 – Splunk Apps

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

Module 4 – Splunk Configuration Files

- Describe Splunk configuration directory structure
- Understand configuration layering process
- Use btool to examine configuration settings

Module 5 – Splunk Indexes

- Learn how Splunk indexes function
- Identify the types of index buckets
- Create new indexes
- Identify the advantages of using multiple indexes
- Monitor indexes with Monitoring Console (MC)

Module 6 – Splunk Index Management

- Manage indexes with Splunk web
- Describe indexes.conf attributes and stanzas
- Customize index retention policies
- Back up indexes
- Delete events from an index
- Restore frozen buckets

Module 7 – Splunk User Management

- Add Splunk users using native authentication
- Describe user roles in Splunk
- Create a custom role
- Splunk authentication options

Module 8 – Configuring Basic Forwarding

- Identify forwarder configuration steps
- List Splunk forwarder types
- Configure the forwarder
- Identify forwarder configuration files

Module 9 – Distributed Search and Splunk Diag

- Describe how distributed search works
- Explain the roles of the search head and search peers
- List search head scaling options
- Describe a Splunk diag
- Generate a Splunk diag

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