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
- Introduction to Splunk Clusters

Course Prerequisites

Required:

- Splunk Fundamentals 1

Strongly Recommended:

- Splunk Fundamentals 2

Class Format

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

Course Modules

Module 1 – Splunk Developer Overview

- Splunk overview
- Identify Splunk components
- Identify Splunk system administrator role

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

- Describe index structure
- List types of index buckets
- Create new indexes
- Monitor indexes with Monitoring Console

Module 6 – Search Head Cluster

- Apply a data retention policy
- Backup data on indexers
- Delete data from an index
- Restore frozen data

Module 7 – Splunk User Management

- Describe user roles in Splunk
- Create a custom role
- Add Splunk users

Module 8 – Splunk Authentication Management

- Integrate Splunk with LDAP
- List other user authentication options
- Describe the steps to enable Multifactor Authentication in Splunk

Module 9 – Getting Data In

- Describe the basic settings for an input
- List Splunk forwarder types
- Configure the forwarder
- Add an input to UF using CLI

Module 10 – Distributed Search

- Describe how distributed search works
- Explain the roles of the search head and search peers
- Configure a distributed search group
- List search head scaling options

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.
270 Brannan
San Francisco, CA
94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com