Splunk Enterprise System Administration

Course Summary:

This course is 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 Duration:

12 Hours

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- Intro to Splunk
- Using Fields
- Intro to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models

Course Outlines:

Module 1 – Deploy Splunk

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- List the steps to install Splunk
- Use Splunk CLI commands
- Explore security best practices

Module 2 – Monitor Splunk

- Use Splunk Health Report
- Enable the Monitoring Console
- Use Splunk Assist
- Use Splunk Diag

Module 3 – License Splunk

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

Module 4 – Use Configuration Files

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

Module 5 – Use Apps

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

Module 6 – Create Indexes

- Learn how Splunk indexes function
- Identify the types of index buckets
- Add and work with indexes
- Overview of metrics index

Module 7 – Manage Index

- Review Splunk Index Management basics
- Identify data retention recommendations
- Identify backup recommendations
- Move and delete index data
- Describe the use of the fishbucket
- Restore a frozen bucket

Module 8 – Manage Users

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

Module 9 – Configure Basic Forwarding

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the deployment server

Module 10 – Configure Distributed Search

- Describe how distributed search works
- Define the roles of the search head and search peers

About Splunk Education:

- Administrators