Course Code: HYSPL04G

Course Title: Splunk Enterprise System Administration

Description:

This 12-hour 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.

Objectives:

- Splunk Deployment Overview
- License Management
- Splunk Configuration Files
- Splunk Apps
- Index Management
- Users, Roles, and Authentication
- Basic Forwarding
- Distributed Search

Prerequisites:

Basic knowledge on Splunk fundamentals

Duration:

12 Hrs

Topics:

Module 1 – Deploying 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 – Monitoring Splunk

- Use Splunk Health Report
- Enable the Monitoring Console (MC)
- Use Splunk Assist
- Use Splunk Diag

Module 3 – Licensing Splunk

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

Module 4 – Using Configuration Files

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

Module 5 – Using Apps

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

Module 6 – Creating Indexes

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

Module 7 – Managing 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 – Managing Users

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

Module 9 – Configuring Basic Forwarding

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the Deployment Server

Module 10 – Configuring Distributed Search

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

Audience:

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification:

None