Course Code: HYSPL02G

Course Title: Architecting Splunk Enterprise Deployments

## Description:

This 9-hour course focuses on large enterprise deployments. Students learn steps and best practices for planning, data collection and sizing for a distributed deployment. Workshop-style labs challenge students to make design decisions about an example enterprise deployment.

## Objectives:

Requirements definition

- Index and resource planning
- Clustering Overview
- Forwarder and Deployment
- Integration
- Performance Monitoring and Tuning
- Use Cases

## Prerequisites:

- Knowledge on Splunk fundamentals.
- Knowledge on Splunk Enterprise Admin.

## Duration:

9 Hrs

## Topics:

Module 1 – Introduction

- Overview of the Splunk deployment planning process and associated tools

Module 2 – Project Requirements

- Identify critical information about environment, volume, users, and requirements
- Review checklists and resources to aid in collecting requirements

Module 3 – Infrastructure Planning: Index Design

- Design and size indexes
- Estimate storage requirements
- Identify relevant apps

Module 4 – Infrastructure Planning: Resource Planning

- List sizing factors for servers

- Describe how reference hardware is used to scale deployments
- Identify the impact of clustering for index replication and for search heads

Module 5- Clustering Overview

- Describe the different clustering capabilities
- Introduce the concepts of indexer and search head clustering

Module 6 - Forwarder and Deployment Best Practices

- Review types of forwarders
- Describe how to manage forwarder installation
- Review configuration management for all Splunk components, using Splunk deployment tools
- Provide best practices for a Splunk deployment

Module 7 - Integration

- Describe integration methods
- Identify common integration points

Module 8 – Performance Monitoring and Tuning

- Use the Monitoring Console to track the performance of your test environment
- List options to fine tune performance for production environment

Module 9 – Use Cases

- Provide example architecture topologies
- Discuss different architecture options based on use case

## Audience:

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

## Certification:

None