Architecting Splunk Enterprise Deployments

Course Description:

This course is for architects and others tasked with implementing and managing large enterprise deployments.

The course covers Splunk deployment planning, Index and resource planning, an overview of Splunk clustering, forwarder selections and forwarder management, integration with other Splunk and third-party products, performance monitoring and tuning, and Splunk use cases.

Course Duration:

2 Days

Prerequisites:

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

- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration
- Troubleshooting Splunk Enterprise

Additional courses and/or knowledge in these areas are also highly recommended:

- Enriching Data with Lookups
- Data Models
- Splunk Enterprise Cluster Administration

Course Outlines:

Module 1 – Splunk Deployment Planning

- Define the responsibilities of a Splunk Architect
- Introduce the Splunk deployment planning process and tools
- Identify the information that is needed for deployment decisions
- Identify use cases
- Provide lists and resources to aid in collecting requirements
- Review the network topology for Buttercup Games

Module 2 – Index Design

- Define index implementation
- Design indexes
- Estimate storage requirements for indexes
- Identify relevant apps and document impact on inputs and indexes

Module 3 – Resource Planning

- Determine sizing based on Splunk usage
- Define reference server requirements for Indexers, Search heads, and other Splunk components
- Describe deployment options such as virtualization and cloud
- Describe the impact of acceleration and apps on resource sizing

Module 4 – Clustering Overview

- Review indexer clustering, including single-site and multi-site clusters
- Define clustering requirements, best practice, and SmartStore
- Review search head clustering
- Defined search head clustering requirements and best practices

Module 5 – Forwarder and Deployment Best Practices

- Review forwarder types
- Manage forwarder installation in an enterprise environment using Deployment Server, Cluster Manager, and SHC Deployer

Module 6 – Integration

- Describe and identify common integration methods

Module 7 – Performance Monitoring and Tuning

- Use the Monitoring Console (MC) to track performance of your test environment before going into production
- Identify options to optimize the production environment
- Overview of Workload Management

Module 8 – Use Cases

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

Target Audience:

- Splunk Enterprise Architects