Splunk Power User and Admin Certification provide in-depth knowledge about the latest concepts which are required for both Splunk Administrators and Splunk Power Users. The training introduces the delegates with the Machine Data and understand the challenges it presents. The delegates will understand how Splunk can be leveraged to gain Operational Intelligence. The delegates will understand how to work with Configuration files and settings, use Searching & Reporting commands, use various Knowledge objects, and finally create Dashboards for visualisation with the help of real-life Use-Cases. The delegates will learn how to setup a Cluster of Splunk instances.

Throughout the training, the delegates will learn how to create and manage users. The delegates will also understand the architecture of Splunk Index and work with Splunk Configuration files. With the help of the training, the delegates will learn the various Splunk Data onboarding techniques and query that data with basic and advanced Splunk commands. The training provides complete knowledge of the schedule alerts, create Reports and Dashboards along with different visualisations. At the end of the Splunk Power User & Admin Certification, the delegates will able to understand their roles and responsibilities.

Prerequisites

There are no prerequisites for attending Splunk Power User & Admin training but it is highly recommended for professionals of analytics domain and IT Operations.

Course Objectives

After the completion of Splunk Power User & Admin Certification at Silicon Beach Training, the delegates will be able:

- Understand Splunk Power User and Admin concepts
- Understand how to apply various Splunk techniques to visualise data using different dashboards and graphs
- Implement Splunk in the organisation to monitor and analyse systems for operational intelligence
- Learn how to configure reports and alerts for monitoring purposes
- Troubleshoot different application logs issues using SPL (Search Processing Language)
- Implement Splunk Indexers, Search Heads, Forwarder, Deployment Servers & Deployers

Introduction to Machine Data and Splunk Basics

- What are Machine Data and its challenges?
- Need for Splunk and its features
- Splunk Products and their Use-Case
- Download and Install Splunk
- Splunk Components: Search Head, Indexer, Forwarder, Deployment Server, & License Master

- Understand the Splunk Architecture
- Splunk Licensing options

User Management and Splunk Configuration Files

- Introduction to Authentication techniques
- User Creation and Management
- Introduction to Indexes
- About the Data Ageing
- Splunk Admin Role & Responsibilities
- Splunk configuration files (7)
- Managing the. conf files

Data Ingestion, Splunk Search, and Reporting Commands

- Understand many data onboarding techniques: -
  - Via flat files
  - Via UF (Universal Forwarder)
- Basic search commands implementation in Splunk: -
- Fields, Rename, Table, Sort, and Search
- Understand the usage of time ranges though searching
- Understand Reporting & Transforming commands in Splunk:-
- Top, Rare, Stats, Chart, Timechart, Dedup and Rex

Knowledge Objects- 1

- Splunk Knowledge
- Categories of Splunk Knowledge
- About fields
- Field extraction
- Event types
- Transactions

Knowledge Objects- 2

- What are lookups?
- Defining a lookup
- Configuring an automatic lookup
- Using the lookup in searches and reports
- About tags
- Workflow action
- Overview of Data Model
- Understand about creating and managing tags
- Defining and searching field aliases

Splunk Alerts, Visualizations, Resorts, and Dashboards

- Create Alerts triggered on certain conditions
- Different Splunk Visualizations
- Create Reports with search results
- Create Dashboards with different Charts and other visualisations

Tel +44 20 4571 2395
info@siliconbeachtraining.co.uk

- Set permissions for Reports and Dashboard
- Create Reports and schedule them using cron schedule
- Share Dashboard with other teams

Splunk Clustering Techniques

- Install Splunk on Linux OS
- Use the frequently used Splunk CLI commands
- Learn the best practices while setting up a Clustering environment
- Introduction to Splunk Clustering
- Implement Search Head Clustering
- Implement Indexer Clustering
- Deploy an App on the Search Head cluster

Splunk Power User and Admin Certification provide in-depth knowledge about the latest concepts which are required for both Splunk Administrators and Splunk Power Users.