**Splunk Developer and Admin**

**Duration: 20 hours**

Splunk, one of the highly used data analysis software is utilized by global organizations for searching, analyzing and monitoring through huge amount of data. Other benefits of Splunk includes report generation, dashboard creation, and visualizing of data on real-time basis. The areas where it is mostly effective, are application management, security and web analytics.

It provides highest-level training in Splunk Developer & Admin for aspiring professionals, with latest course-ware covering in-depth knowledge and skill enhancement in Splunk implementation. Other features of Splunk certification training includes Splunk Basics, Licensing, Setting up Splunk Search head, Splunk Admin roles and more.

**The Splunk Developer and Admin training program also imparts about:**

* Splunk development concepts
* Splunk Basic search queries
* Coordinating with Splunk Support
* Conditional statements
* Defining event types and their usefulness
* Defining a lookup

**Target Audience**

* System Administrators
* Software Developers
* Analytics Managers
* Individual Contributors/Architects willing to implement Splunk in their organizations

**Prerequisites**

* Basic knowledge in SQL queries and command line interface.

**1.Splunk Basics, Licensing and Configuration Files**

* Introduction to the course
* What is Splunk?
* Prerequisites
* Setting up Splunk search head, indexer
* Setting up Splunk forwarder
* Splunk Licensing, Configuration files on Linux
* Configuration files on Windows
* Difference between Linux and Windows OS in Splunk configuration
* Types of files supported in Splunk: Common Splunk configuration files, Configuring inputs.conf and outputs.conf, Configuring props.conf, Configuring index.conf, Configuring savedsearches.conf

**2. Managing Users, Indexes, Splunk Admin Roles and Clustering**

* User creation and management
* Managing indexes
* Importance of roles
* Different permissions of each indexes
* Splunk development concepts
* Roles and responsibilities of Splunk Developer
* How to configure LDAP authentication in Splunk
* Admin role in managing Splunk
* What is alert?
* Reports and dashboards
* Coordinating with Splunk Support
* Implement Search Head Clustering
* Implement Indexer Clustering

**3. Splunk Search Commands and Reporting Commands**

* Different keywords
* Splunk Basic search queries and using various commands to perform searches: fields, table, rename,
* rex&erex, multikv
* Usage of following commands and their functions: Top, Rare, Stats, Addcoltotals, Addtotals
* Explore the available visualizations
* Creation of charts and timecharts
* Omit null values and format results

**4. Deployment Process, Alerts, Tags and Event Types**

* Deploy Apps using Deployment server
* creating tags and using them in search
* Defining event types and their usefulness
* Creating and using event types in search
* creating and modifying alerts and use of Alerts

**5. Analyzing & Calculating Results, Fields Extraction and Lookups**

* Using eval command
* Perform calculations
* Value Conversion
* Round values
* Format values
* Conditional statements
* Filtering calculated results
* Raw Data Manipulation
* Extraction of Fields,
* What are lookups?
* Lookup file example
* Creating a lookup table
* Defining a lookup
* Configuring an automatic lookup
* Using the lookup in searches and reports

**6. Splunk Visualizations, Reports and Dashboards**

* Explore the available visualizations
* Creating reports and charts
* Creating dashboards and adding reports

**7. Ansible for Splunk Config**

* Installing Ansible
* Ansible Structure
* Roles
* Running Ansible
* Deploying Splunk Securely