Adv Splunk Training

Customized Course Contents

Duration
05 days

Delivery Format
08 hours per day

Pre-requisites for attending this training: Participants should have prior knowledge in:

1. Basic Linux commands
2. Basic understanding on Machine learning

Course Overview

This five-day Advanced Splunk Training course offers a comprehensive deep dive into Splunk's capabilities, covering installation, data analytics, MLTK implementation, system administration, and dashboard creation.

Course Objectives

- **Master Splunk Fundamentals**: Understand the core functionalities of Splunk, from basic installation to real-time data processing.
- **Data Handling and Analysis**: Learn to input, search, report, and analyze data effectively using Splunk's powerful commands and features.
- **Implement Machine Learning**: Explore machine learning algorithms within Splunk to enhance data predictions and analytics.
- **System Administration Skills**: Gain essential skills in Splunk system administration, including license management, system architecture, and troubleshooting.
- **Develop and Manage Splunk Applications**: Learn to create, configure, and manage Splunk apps and add-ons to extend functionality.
- **Dashboard and Visualization Expertise**: Craft dynamic, data-driven dashboards and integrate advanced visualization techniques.

Target Audience

This course is designed for IT professionals with basic Linux and machine learning knowledge, aiming to master Splunk for enhanced data analytics and system management.

Day-wise Course Outline

Splunk - Table of Contents (05 Full Days)		
Day	Module	Topics
Day - 1	Module - 1	What is Splunk
		How Splunk Started
		Splunk Overview
		Splunk Real Time Examples – Windows, Linux and Apache IIS Logs
		Splunk Deployment Methods
		Splunk Installation Lab
	Module - 2	Data Input in Splunk
		Splunk UI Overview
		Creating and scheduling searches
		Demo - Searches
		Creating and scheduling Alerts
		Demo - Alerts
		Splunk Alert Integration with Multiple tools
		Lab on Module 2
Day - 2	Module - 3	Splunk searches and reporting commands
		stats
		field
		table
		rex
		rename
		where
		top
		rare
		Join
		addcoltotals
		chart
		timechart
		Eventcount
Day - 3	Module - 4	Splunk Knowledge objects
		saved searches
		event types

		tags
		field extractions
		lookups
		reports
		alerts
		Transactions
		data model
		fields
		workflow actions
	Module - 5	Enriching Data with Lookups
		Correlating Events
		Analysing, Calculating and Formatting Results
		Data Model Implementation
		Performance Improvement Splunk Queries
		Best practice for Splunk Queries
	Module - 6	Predict Command
		Local level (LL) Algorithm
		Local level trend (LLT) Algorithm
		Seasonal local level (LLP) Algorithm
		LLP5 Algorithm
		Bivariate local level (LLB) Algorithm
		Bivariate local level (BiLL) Algorithm
Day - 4	**Module - 7**	Splunk MLTK ToolKit
		Install Splunk MLTK
		Implementation of Linear Regression in Splunk MLTK
		Deep Dive into Splunk MLTK Commands for LR
		Splunk DLKT Setup
	Module - 8	Splunk System Administration
		Splunk Deployment Overview
		Splunk Engine Architecture
		Splunk Deployment Architecture
	Module - G	Splunk License Management
		Splunk License Types
		License Warnings and Violations

		Add and Remove Licenses
		Splunk License Master-Slave setup
		Splunk License Pools
	Module - 10	Splunk Apps & Add-Ons
		Concept and Pre-Requisites
		Installation and Configuration
		Fine-tuning and Uninstallation
		Creating a Sample Splunk App
	Module - 11	Splunk Indexes
		Concept of Splunk Indexes
		Splunk Index structure
		Create and configure new Indexes (UI, CLI C Conf file methods)
		Monitor Splunk Indexes using MC
Day - 5	**Module - 12**	Classic Dashboard Creation
		Static Dashboard Creation
		Dynamic Dashboard Creation
		Conditional Statement
		Integration of JS with Classic Dashboard
		Optimization of Dashboard
		Splunk Studio Dashboard
	Module - 13	DB Connect
		Batch Process
		Rising Column
		Data Ingestion
	Module - 14	Data Ingestion for Linux Server
		Windows Server data onboarding
	Module - 15	Closure
		Notes