Splunk Admin and Cluster Management - 5-Day Training

Day 1: Introduction to Splunk & Installation

- Introduction to Splunk
- Overview of Splunk
- Splunk Architecture and Components
- Deployment Models (Standalone, Distributed, Clustered)
- Installation & Setup
- System Requirements
- Splunk Installation (Windows/Linux)
- Basic Configuration and First-Time Setup
- User Authentication and Access Control
- Splunk Licensing & Data Inputs
- Splunk License Types
- Adding Data to Splunk (File, Syslog, API, Database)
- Indexing and Parsing Mechanism
- Troubleshooting Data Onboarding Issues

Day 2: Splunk Configuration & Index Management

- Splunk Configuration Files
- Important Splunk Configuration Files
- Configuration File Precedence
- Managing and Modifying Configuration Files
- Index Management
- Understanding Indexing
- Creating & Managing Indexes

- Hot, Warm, Cold & Frozen Buckets
- Data Retention and Archiving Policies
- Best Practices for Index Performance Optimization
- User & Role Management
- Splunk User Authentication
- Role-Based Access Control (RBAC)
- Creating & Managing Users/Roles
- Assigning Permissions and Capabilities
- LDAP & SAML Integration

Day 3: Splunk Forwarders & Deployment Server

- Forwarders & Data Collection
- Splunk Universal Forwarder vs. Heavy Forwarder
- Forwarder Installation & Configuration
- Configuring Forwarders for Log Forwarding
- Troubleshooting Forwarder Connectivity
- Splunk Deployment Server
- Introduction to Deployment Server
- Managing Forwarders with Deployment Server
- Configuring Server Classes
- Rolling Out Configurations to Forwarders
- Monitoring Deployment Server Status
- Search Head Clustering
- Introduction to Search Head Clustering
- Deploying and Configuring Search Head Cluster
- Synchronization of KV Stores

- Troubleshooting Cluster Issues

Day 4: Splunk Indexer & Cluster Management

- Indexer Clustering
- Introduction to Indexer Clustering
- Single-Site vs Multi-Site Clustering
- Configuring Indexer Cluster
- Understanding Cluster Master (CM) Role
- Replication & Search Factor
- Load Balancing & High Availability
- Configuring Load Balancing in Splunk
- Data Replication for High Availability
- Best Practices for Cluster Performance
- Troubleshooting Common Issues in Clusters
- Monitoring & Performance Optimization
- Using Splunk Monitoring Console
- Identifying Bottlenecks & Performance Tuning
- Monitoring Splunk Logs & System Health
- Splunk Data Lifecycle & Storage Optimization

Day 5: Advanced Topics & Troubleshooting

- Advanced Configuration
- Distributed Deployment Management
- Configuring Splunk in Cloud vs. On-Prem
- Splunk App & Add-on Management
- Advanced Search & Reporting
- Overview of Splunk Search Language (SPL)

- Creating Advanced Dashboards & Reports
- Data Model & Accelerations
- Troubleshooting & Best Practices
- Troubleshooting Common Splunk Issues
- Debugging Errors & Log Analysis
- Best Practices for Admins & Cluster Management
- Security Best Practices for Splunk Environments