Splunk Admin Basic to Advance

1. Introduction to Splunk

1.1 What is Splunk?

- Overview of Splunk
- Key Features and Use Cases

1.2 Splunk Architecture

- Core Components: Forwarder, Indexer, Search Head
- Data Flow in Splunk
- Deployment Types: Single Instance, Distributed, Clustered

1.3 Installation and Setup

- Installing Splunk on Windows, Linux, and macOS
- Splunk Licensing: Free vs. Enterprise
- Initial Configuration: Inputs, Outputs, and Indexes

2. Data Input and Forwarding

2.1 Adding Data to Splunk

- Input Types: Files, Directories, TCP/UDP, Syslog
- Configuring Data Inputs

2.2 Forwarders

- Universal Forwarder vs. Heavy Forwarder
- Installing and Configuring Forwarders
- Monitoring and Managing Forwarders

2.3 Data Parsing and Indexing

- Data Parsing Process: Line Breaking, Timestamping, Event Typing
- Understanding Indexes: Hot, Warm, Cold, Frozen Buckets
- Configuring Indexing (indexes.conf)

3. Search Processing Language (SPL)

3.1 Basic Search Commands

- Search Command Syntax
- Using Fields, Tables, and Statistics
- Filtering and Sorting Results

3.2 Advanced Search Techniques

- Subsearches and Joins
- Transactions and Correlation
- Using Lookups and Field Extractions

3.3 Search Optimization

- Best Practices for Efficient Searches
- Using Search Job Inspector
- Accelerated Searches and Summary Indexing

4. Data Management

4.1 Index Management

- Creating and Managing Indexes
- Index Retention Policies

- Data Aging and Archiving

4.2 Data Onboarding and Transformation

- Best Practices for Data Onboarding
- Data Enrichment and Normalization (props.conf, transforms.conf)
- Using Common Information Model (CIM)

4.3 Managing Splunk Data Integrity

- Data Integrity Checks
- Handling Corrupted or Missing Data
- Implementing Data Security and Privacy Measures

5.. User and Role Management

5.1 User Authentication

- Managing Local Users
- Integrating with LDAP, SAML, and Other Authentication Systems

5.2 Role-Based Access Control (RBAC)

- Creating and Assigning Roles
- Managing Permissions and Capabilities
- Index-level Access Control

5.3 Managing Multi-Tenancy in Splunk

- Setting Up Multi-Tenant Environments
- Data and Resource Segmentation

7. Distributed Search and Clustering

7.1 Distributed Search Configuration

- Overview of Distributed Search
- Configuring Search Peers and Search Heads
- Managing Distributed Search Performance

7.2 Search Head Clustering

- Introduction to Search Head Clustering
- Setting Up and Managing Clusters
- Dealing with Cluster Failures and Data Recovery

7.3 Indexer Clustering

- Introduction to Indexer Clustering
- Configuring Peer Nodes and Master Node
- Monitoring and Troubleshooting Clusters

8. Monitoring and Maintaining Splunk

8.1 Monitoring Splunk Deployments

- Using the Monitoring Console
- Monitoring Splunk Logs and Performance Metrics
- Setting Up Health Checks and Alerts

8.2 Performance Tuning

- Optimizing Search Performance
- Managing Resource Utilization (CPU, Memory, Disk I/O)
- Best Practices for Scaling Splunk

8.3 Backup and Disaster Recovery

- Implementing Backup Strategies
- Disaster Recovery Planning
- Data Restoration and Failover Procedures

9. Advanced Splunk Administration

9.1 Splunk Apps and Add-Ons

- Installing and Configuring Splunk Apps
- Developing Custom Apps and Add-Ons
- Managing App Deployment across Environments

9.2 Integrating Splunk with External Systems

- Integrating with Cloud Platforms (AWS, Azure, GCP)
- Using REST API for Automation

10. Splunk Cloud Administration

10.1 Splunk Cloud vs. On-Premises

- Key Differences and Considerations
- Setting Up and Managing Splunk Cloud

11. Troubleshooting and Best Practices

11.1 Common Troubleshooting Techniques

- Troubleshooting Data Ingestion Issues
- Search and Reporting Issues
- Dealing with Performance Bottlenecks

11.2 Splunk Best Practices

- Configuration Management
- Documentation and Knowledge Sharing
- Keeping Splunk Up-to-Date and Secure

11.3 Community and Support Resources

- Using Splunk Documentation and Community Forums
- Engaging with Splunk Support
- Participating in Splunk User Groups and Conferences