jotHUB

SPLUNK

ADMINISTRATION ADVANCED CLUSTERING DEVELOPMENT

Ambadasu kiran

Course Curriculum

1 INTRODUCTION TO SPLUNK

2 INTRODUCTION TO SPLUNK COMPONENTS

3 SEARCH MODES IN SPLUNK

4 SPLUNK ENVIRONMENT SETUP

5 IN-DEPTH OF SPL CONCEPTS

6 FIELD EXTRACTIONS

7 KNOWLEDGE OBJECTS

8 SPLUNK ADMIN - REAL-TIME SCENARIOS AND DEPLOYMENTS

MODULE'S

01 INTRODUCTION TO SPLUNK

— Overview of Log Management Tools in the Market
— Splunk vs. ELK: Comparative Analysis
— Splunk vs. Other Tools
— Key Features & Strengths of Splunk
— Splunk Architecture and Ecosystem Overview
— Types of Data Ingested by Splunk
— Understanding the Splunk File System
— Introduction to Splunkbase and Enhanced Solutions

02 INTRODUCTION TO SPLUNK COMPONENTS

— Search Head
— Indexer
— Universal Forwarder
— Heavy Weight Forwarder
— Heavy Weight Forwarder
— Load Balancing with Multiple Indexers
— Deployment Server
— Cluster Master
— Index Cluster
— Deployer
— License Managerr

03 SEARCH MODES IN SPLUNK

— Fast Mode

— Smart Mode

— Verbose Mode

04 SPLUNK ENVIRONMENT SETUP

— Hardware Requirements

— Splunk Installation (Standalone & Distributed)

— Creating AWS/GCP Instances

— SSH Access to Instances

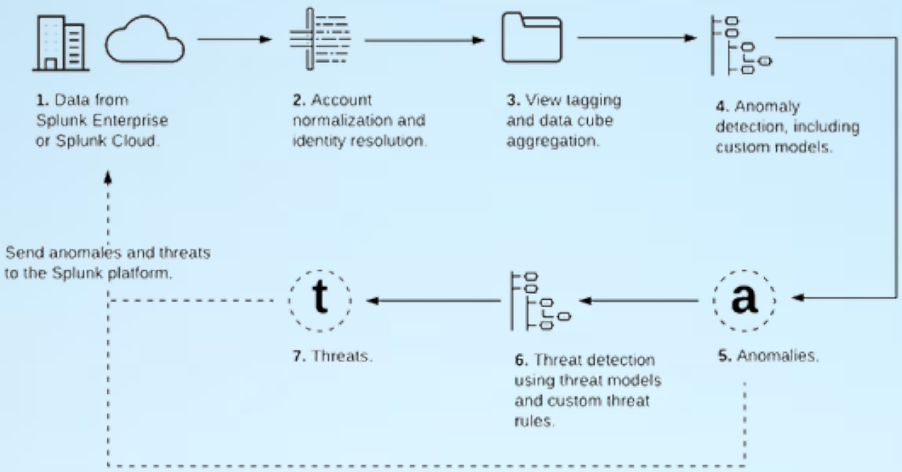
— Essential Linux Commands for Splunk Admins

– Splunk Directory Structure Overview

— Commonly Used Configuration Files & Their Precedence

— Understanding Splunk Licensing Models

— Key Ports Used in Splunk Environment



05 IN-DEPTH OF SPL (SEARCH PROCESSING LANGUAGE) CONCEPTS

Search Basics

— Search Terms and Commands
— Search Performance Optimization
— Search Jobs and Execution Flow
— Working with Search Results
— Filtering & Non-Transforming Commands

Filtering & Non-Transforming Commands

— table
— fields
— dedup
— head
— tail
— reverse
— rename
— replace
— sort
— search

Transforming Commands

— top

— rare

— stats

— chart

— timechart

— eval

— logical operators (AND, OR, NOT)

Advanced SPL Commands

— stats

— eventstats

— streamstats

— geostats

— tstats

— addtotals

— addcoltotals

— join and subsearch usage

Power of Splunk
Search Processing Language
(SPL™)

06 FIELD EXTRACTIONS

— Index-time field extractions

— Search-time field extractions

— Index-Time vs. Search-Time Field Extractions

FIELD EXTRACTION METHODS

— GUI based Field extractions

— Regular Expressions

— Props and transformation configurations

— Rex and regex commands

— Centralized Extraction via Deployment Server

07 KNOWLEDGE OBJECTS

1

- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Data models

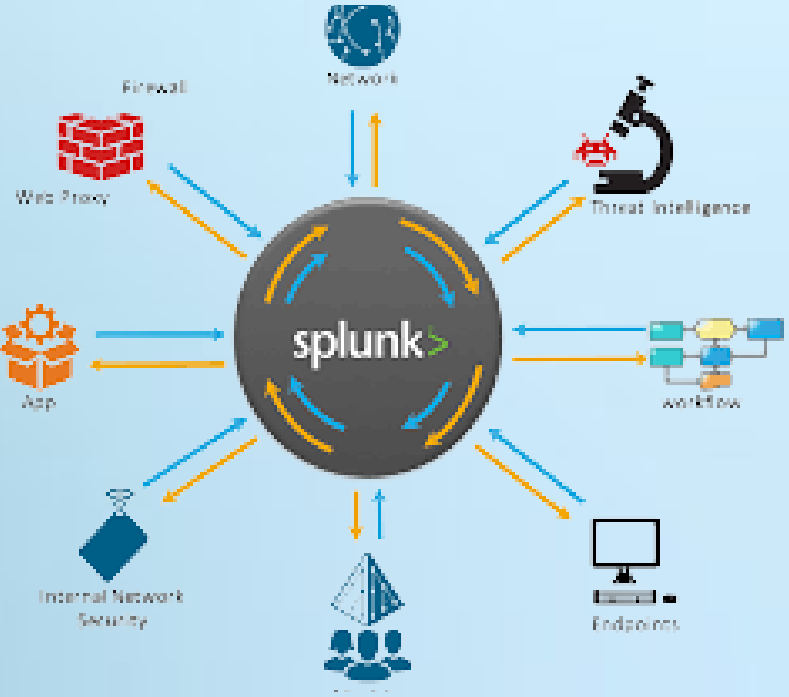
2

- chart types
- Lookups
- KV Store Collections
- Alerts
- Reports
- All configurations
- Advanced search
- Macros
- Visualisations

3

- Dashboards
- Apps and addons
- Workflows and aliases
- Data models
- Data sets
- pivots
- Searches, reports, and alerts

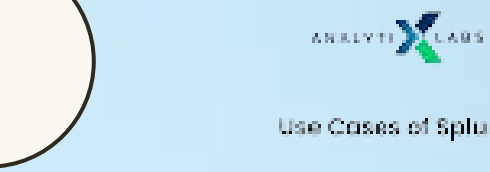
08 SPLUNK ADMIN - REAL-TIME SCENARIOS AND DEPLOYMENTS



SPLUNK BASIC AND ADVANCED COMPONENT DEPLOYMENTS ON CLOUD (AWS/ GCP):

— Universal Forwarder
— Heavy Forwarder
— Indexer
— Searchhead
— Deployment Server
— Cluster Master
— Index Cluster
— Searchhead Cluster
— Deployer
— License Master

NOTE: DEPLOYMENT SCENARIOS OF SPECIFIED COMPONENTS ARE PROVIDED IN ALL 3 DIFFERENT MODES:
A. WEB INTERFACE
B. COMMAND LINE INTERFACE
C. CONFIGURATION FILES



— User Management and Authentication
— In-depth of Data storage mechanism
— Data Life stages in Splunk
— Typical Ingestion Flow
— Creating real time setup for Data Onboarding
— Creating real time setup for Deployment Server
— Creating real time setup for Clustered Environment(Cluster Master,Index&shCluster)
— Creating real time setup for Deployer Environment with SH Cluster

*Each topic is supplemented with practical oriented sessions,use-case discussions, and real-world problem-solving techniques along with daily class recordings to ensure practical learning and operational confidence.

MORE DETAILS

Contact:

+91 75695 80831, +91 99599 64770
+91 99599 64770(whatsapp)
splunkonlinetutorials@gmail.com