Day1

Using Splunk 6.4

Chapter	Topic	Sub Topic
Introduction to Big Data	What is Big Data?	Introduction
Introduction to Big Data	What do we gain from Big Data?	Gains
Introduction to Big Data	How Big Data Tool Helps?	4 V's, Needle in Hey Stack
Introduction to Big Data	Hadoop/MapReduce	High Level Overview/History
Introduction to Big Data	Hadoop/MapReduce	How Map Reduce Works
Installation	Install Splunk	Single Machine Installation
Architecture	Splunk components that allow inputs, indexing, and searching	Forwarder, Indexer, Search Head
Architecture	Splunk's application framework	Overview
Architecture	Splunk's development platform	Overview
Architecture	Distributed Architecture Overview	Building Splunk Cluster
Using Splunk	Walk Through the Interface	Overview
Using Splunk	Define Splunk Apps	Apps Overview
Using Splunk	Understand the lab environment	Explain Test company & the data associated
Session2		
Using Splunk	Getting Data Into Splunk	File or Directory of Files
Using Splunk	Getting Data Into Splunk	Syslog, Network Ports(UDP/TCP)
Using Splunk	Getting Data Into Splunk	Windows Event Log, Registry
Using Splunk	Getting Data Into Splunk	Windows PerfMon/WMI
Using Splunk	Getting Data Into Splunk	IIS, Apache, Web Access, Middleware logs
Using Splunk	Splunk Programming Language Introduction	Run basic searches
Using Splunk	Splunk Programming Language Introduction	Set the time range of a search
Using Splunk	Splunk Programming Language Introduction	Identify the contents of search results
Using Splunk	Splunk Programming Language Introduction	Refine searches
Using Splunk	Splunk Programming Language Introduction	Use the timeline
Using Splunk	Splunk Programming Language Introduction	Save search results

Day-2

Chapter	Topic	Sub Topic
Using Splunk	SPL Advance	Using search commands: fields, table, rename, rex
Using Splunk	SPL Advance	Using search functions: stats, top, head, addtotals
Using Splunk	SPL Advance	Performing calculation Using eval
Using Splunk	Correlating Events	Group Events using fields/Time
Using Splunk	Correlating Events	Using Transaction command
Using Splunk	Lookups	Describe lookups
Using Splunk	Lookups	Examine a lookup file example
Using Splunk	Lookups	Create a lookup table
Using Splunk	Lookups	Define a lookup
Using Splunk	Lookups	Configure an automatic lookup
Using Splunk	Lookups	Use the lookup in searches and reports
Session2		
Using Splunk	Using Fields	Understand fields
Using Splunk	Using Fields	Use fields in searches
Using Splunk	Using Fields	Use the fields sidebar
Using Splunk	Using Fields	Use search modes (fast, verbose, and smart)
Using Splunk	Creating Reports	Save a search as a report
Using Splunk	Creating Reports	Edit reports
Using Splunk	Creating Reports	Create reports that include Visualizations
Using Splunk	Creating Dashboards	Create New Dashboard
Using Splunk	Creating Dashboards	Add Reports to Dashboard

Day3

Using Splunk	Creating Pivot/Data Model	Describe Pivot
Using Splunk	Creating Pivot/Data Model	Understand the relationship between data models and pivot
Using Splunk	Creating Pivot/Data Model	Select a data model object
Using Splunk	Creating Pivot/Data Model	Create a pivot report
Session2		
Using Splunk	Creating and Using Macros	Describe macros

Using Splunk	Creating and Using Macros	Manage macros
Using Splunk	Creating and Using Macros	Create and use a basic macro
Using Splunk	Creating and Using Macros	Define arguments and variables for a macro
Using Splunk	Creating and Using Macros	Add and use arguments with a macro
Using Splunk	Creating and Managing Alerts	Describe alerts
Using Splunk	Creating and Managing Alerts	Create alerts
Using Splunk	Creating and Managing Alerts	View fired alerts
Day4		
Build Custom Apps	Getting started	Define Splunk apps
Build Custom Apps	Getting started	Describe views in the context of apps
Build Custom Apps	Getting started	Explain knowledge objects in the context of apps
Build Custom Apps	Getting started	Describe roles & permissions for apps
Build Custom Apps	Create your app	Define the steps to create an app
Build Custom Apps	Create your app	Explain how to use app builder
Build Custom Apps	Create your app	Describe the two app templates
Build Custom Apps	Create your app	Identify app knowledge objects
Build Custom Apps	Create your app	Create a view
Build Custom Apps	Create your app	Set view and app permissions
Build Custom Apps	Add configurations	Describe how configuration files relate to apps
Build Custom Apps	Add configurations	Identify where to change config settings
Build Custom Apps	Add configurations	Learn stanza and attributes of config files
Build Custom Apps	Add objects	Explain how to access a view's simple XML

Build Custom Apps	Add objects	Identify the simple XML panel objects
Build Custom Apps	Add objects	Define the simple XML syntax
Build Custom Apps	Add objects	Modify panels using simple XML
Session2		
Build Custom Apps	Build Navigation for your App	Create navigation for an app
Build Custom Apps	Build Navigation for your App	Assign an app icon for the app menu and home page
Build Custom Apps	Build Navigation for your App	Identify two locations for graphic files in an app
Build Custom Apps	Set permissions	Assign permissions to specific user for App access
Day5		
Administration	Configure/Manage Indexer	Set up multiple indexes
Administration	Configure/Manage Indexer	Remove indexes and data from Splunk
Administration	Configure/Manage Indexer	Configure index storage
Administration	Configure/Manage Indexer	Move the index database
Administration	Configure/Manage Indexer	Use multiple partitions for index data
Administration	Configure/Manage Indexer	Configure index size
Administration	Configure/Manage Indexer	Set limits on disk usage
Administration	Configure/Manage Indexer	Back up indexed data
Administration	Configure/Manage Indexer	Set a retirement and archiving policy
Session2		
Administration	Configure/Manage Forwarders	Set up forwarding and receiving
Administration	Configure/Manage Forwarders	Enable a receiver

Administration	Configure/Manage Forwarders	Consolidate data from multiple machines
Administration	Configure/Manage Forwarders	Set up load balancing

Troubleshooting Splunk

- ✓ Splunk Enterprise log files
- ✓ What Splunk logs about itself
- ✓ Enable debug logging
- ✓ About metrics.log
- ✓ Troubleshoot inputs with metrics.log
- ✓ About access logs