Splunk 7.2 Fast Start Training

Splunk Fundamentals 2

Module 1 – Introduction

§ Overview of Buttercup Games Inc.

§ Lab environment

Module 2 – Beyond Search Fundamentals

§ Search fundamentals review

§ Case sensitivity

§ Using the job inspector to view search performance

Module 3 – Using Transforming Commands for Visualizations

§ Explore data structure requirements

§ Explore visualization types

§ Create and format charts and timecharts

Module 4 – Using Mapping and Single Value Commands

§ The iplocation command

§ The geostats command

§ The geom command

§ The addtotals command

Module 5 –Filtering and Formatting Results

§ The eval command

§ Using the search and where commands to filter results

§ The filnull command

Module 6 – Correlating Events

§ Identify transactions

§ Group events using fields

§ Group events using fields and time

§ Search with transactions

§ Report on transactions

§ Determine when to use transactions vs. stats

Module 7 – Introduction to Knowledge Objects

§ Identify naming conventions

§ Review permissions

§ Manage knowledge objects

Module 8 – Creating and Managing Fields

§ Perform regex field extractions using the Field Extractor (FX)

§ Perform delimiter field extractions using the FX

Module 9 – Creating Field Aliases and Calculated Fields

§ Describe, create, and use field aliases

§ Describe, create and use calculated fields

Module 10 – Creating Tags and Event Types

§ Create and use tags

§ Describe event types and their uses

§ Create an event type

Module 11 – Creating and Using Macros

§ Describe macros

§ Create and use a basic macro

§ Define arguments and variables for a macro

§ Add and use arguments with a macro

Module 12 – Creating and Using Workflow Actions

§ Describe the function of GET, POST, and Search workflow actions

§ Create a GET workflow action

§ Create a POST workflow action

§ Create a Search workflow action

Module 13 – Creating Data Models

§ Describe the relationship between data models and pivot

§ Identify data model attributes

§ Create a data model

§ Use a data model in pivot

Module 14 – Using the Common Information Model (CIM)

Add-On

§ Describe the Splunk CIM

§ List the knowledge objects included with the Splunk CIM

Add-On

§ Use the CIM Add-On to normalize data

Splunk Enterprise System Administration

This course is designed for system administrators who are responsible for managing the Splunk Enterprise environment. The course provides the fundamental knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components.

Module 1 – Splunk Deployment Overview

§ Splunk overview

§ Identify Splunk components

§ Identify Splunk system administrator role

§ Identify Splunk installation steps

§ Use Splunk CLI

§ Enable the Monitoring Console (MC)

Module 2 – License Management

§ Identify license types

§ Describe license violations

§ Add and remove licenses

Module 3 – Splunk Apps

§ Describe Splunk apps and add-ons

§ Install an app on a Splunk instance

§ Manage app accessibility and permissions

Module 4 – Splunk Configuration Files

§ Describe Splunk configuration directory structure

§ Understand configuration layering process

§ Use btool to examine configuration settings

Module 5 – Splunk Indexes

§ Understand how indexes function

§ Understand the types of index buckets

§ Create new indexes

§ Explain the advantages of using multiple indexes

§ Monitor indexes with Monitoring Console

Module 6 – Splunk Index Management

§ Manage indexes with Splunk web

§ Describe indexes.conf attributes and stanzas

§ Customize index retention policies

§ Delete events from an index

§ Restore frozen buckets

Module 7 – Splunk User Management

§ Add Splunk users using native authentication

§ Describe user roles in Splunk

§ Create a custom role

§ Splunk authentication options

Module 8 – Configuring Basic Forwarding

§ Identify forwarder configuration steps

§ List Splunk forwarder types

§ Configure the forwarder

§ Identify forwarder configuration files

Module 9 – Distributed Search

§ Describe how distributed search works

§ Explain the roles of the search head and search peers

§ Configure a distributed search group

§ List search head scaling options

Splunk Enterprise Data Administration

This course is designed for system administrators who are responsible for getting data into Splunk Indexers. The course provides the fundamental knowledge of Splunk forwarders and methods to get remote data into Splunk indexers. It covers installation, configuration, management, monitoring, and troubleshooting of Splunk forwarders and Splunk Deployment Server components.

Module 1 – Introduction to Data Administration

§ Splunk overview

§ Identify Splunk data administrator role

Module 2 – Getting Data In – Staging

§ List the four phases of Splunk Index

§ List Splunk input options

§ Describe the band settings for an input

Module 3 – Configuring Forwarders

§ Understand the role of production Indexers and Forwarders

§ Understand the functionality of Universal Forwarders and Heavy Forwarders

§ Configure Forwarders

§ Identify additional Forwarder options

Module 4 – Forwarder Management

§ Explain the use of Forwarder Management

§ Describe Splunk Deployment Server

§ Manage forwarders using deployment apps

§ Configure deployment clients

§ Configure client groups

§ Monitor forwarder management activities

Module 5 – Monitor Inputs

§ Create file and directory monitor inputs

§ Use optional settings for monitor inputs

§ Deploy a remote monitor input

Module 6 – Network and Scripted Inputs

§ Create network (TCP and UDP) inputs

§ Describe optional settings for network inputs

§ Create a basic scripted input

Module 7 – Agentless Inputs

§ Identify Windows input types and uses

§ Understand additional options to get data into Splunk

HTTP Event Collector

Splunk App for Stream

Module 8 – Fine Tuning Inputs

§ Understand the default processing that occurs during input phase

§ Configure input phase options, such as sourcetype fine- tuning and character set encoding

Module 9 – Parsing Phase and Data

§ Understand the default processing that occurs during parsing

§ Optimize and configure event line breaking

§ Explain how timestamps and time zones are extracted or assigned to events

§ Use Data Preview to validate event creation during the parsing phase

Module 10 – Manipulating Raw Data

§ Explain how data transformations are defined and invoked

§ Use transformations with props.conf and transforms.conf to:

Mask or delete raw data as it is being indexed

Override sourcetype or host based upon event values

Route events to specific indexes based on event content

Prevent unwanted events from being indexed

§ Use SEDCMD to modify raw data

Module 11 – Supporting Knowledge Objects

§ Create field extractions

§ Configure collections for KV Store

§ Manage Knowledge Object permissions

§ Control automatic field extraction

Module 12 – Creating a Diag

§ Identify Splunk diag

§ Using Splunk diag