SPLUNK Development

Duration

3 days

Contents

Module 1 – Basic Understanding of Architecture

- What are the components
- Discussion on Forwarders- UF/HF
- Common ports for the set up
- License Master/Slave relationship
- Understanding of Deployment Server and Indexer

Module 2 – Introduction to Splunk's User Interface

- Understand the uses of Splunk
- Define Splunk Apps
- Learn basic navigations in Splunk

Module 3 – Searching

- Run basic searches
- Set the time range of a search
- Identify the contents of search results
- Refine searches
- Use the timeline
- Work with events
- Control a search job
- Save search results

Module 4 – Using Fields in Searches

- Understand fields
- Use fields in searches
- Use the fields sidebar

Module 5 – Creating Reports and Visualizations

- Save a search as a report
- Edit reports
- Create reports that include visualizations such as charts and tables
- Add reports to a dashboard

Module 6 – Working with Dashboards

- Creating a dashboard
- Add a reports to a dashboard
- Add a pivot report to a dashboard
- Edit a dashboard

Module 7 – Search Fundamentals

- Review basic search commands and general search practices

- Examine the anatomy of a search
- Use the following commands to perform searches:
  - Fields
  - Table
  - Rename
  - Rex
  - Multikv

Module 8 – Reporting Commands, Part 1

- Use the following commands and their functions:
  - Top
  - Rare
  - Stats
  - Addcoltotals

Module 9 – Reporting Commands, Part 2

- Explore the available visualizations
- Create a basic chart
- Split values into multiple series
- Omit null and other values from charts
- Create a timechart
- Chart multiple values on the same timeline
- Format charts
- Explain when to use each type of reporting command

Module 10 – Analyzing, Calculating and formatting Results

- Using the eval command:
  - Perform calculations
  - Convert values
  - Round values
  - Format values
  - Use conditional statements
- Further filter calculated results

Module 11 – Creating Field Aliases and Calculated Fields

- Define naming conventions
- Create and use field aliases
- Create and use calculated fields

Module 12 – Creating Field Extractions

- Perform field extractions using Field Extractor

Module 13 – Creating Tags and Event Types

- Create and use tags
- Describe event types and their uses
- Create an event type

Module 14 – Creating Workflow Actions

- Describe the function of a workflow action
- Crate a GET workflow action
- Crate a POST workflow action
- Crate a Search workflow action

Module 15 – Creating and Managing Alerts

- Describe alerts
- Create alerts
- View fired alerts

Module 16 – Creating and Using Macros

- Describe macros
- Manage macros
- Create and use a basic macro
- Define arguments and variables for a macro
- Add and use arguments with a macro

Lab Setup

- ✓ RAM -- 4-8 GB. HDD - 10 GB on both Faculty and Participants machine
- ✓ Base machine OS : Windows with the latest Chrome installed
- ✓ Virtual machine OS : Redhat 6.x with the latest Firefox installed
- ✓ Every Base machine should have 1 virtual machine installed with Splunk software downloaded (NOT Installed) → Version : 6.5.3
- ✓ https://www.splunk.com/en_us/download/splunk-enterprise-2.html#tabs/linux
- ✓ Select “Linux” and download “.tgz” file
- ✓ Port 8000, 8089 and 9997 should be open in all VMs and Base machine
- ✓ External sites like Google, LinkedIn, splunkgeek.blogspot.in should be open
- ✓ Putty, SuperPutty and WinSCP have to be installed and configured in the Base machine so that VMs can be easily accessible from the Base Machine (Windows)
- ✓ Internet should be there in the VM as well as Base machine
- ✓ Minimum bandwidth to perform the network action without fail
- ✓ All VMs should have static IP OR dynamic IP with lease more than 10 days along with unique hostname
- ✓ Need a projector with dual display , white board and marker (blue, black, green)