SPLUNK Administration

Duration

3 days

Prerequisite

- ✓ Candidates should have basic of Linux Fundamental
- ✓ They should thorough with the Linux Environment and the Commands

Contents

Module 1: Installing Splunk

- Splunk: What does it Mean
- How should Splunk be Configured
- Identifying Splunk Instance Types
- Hardware Recommendations Indexers
- Hardware Recommendations Search Heads
- Splunk Install Packages
- Supported Platforms and Browsers
- Splunk Installation
- Splunk Directory Structure
- The Splunk Command Line Interface
- *NIX Run Splunk at Boot
- Splunk Windows Services
- Splunk Processes : Splunkd
- Splunk Processes :Splunk Web
- Apps Installed by Default
- System Settings
- Describing General Settings
- Restarting the Server from Splunk Web

Module 2: License Management

- Managing Licenses
- Splunk License Types
- Adding a License
- License Warnings and violations
- What Counts As Daily License Quota
- Viewing Alerts
- License Staking
- Master License Server
- License Pooling

Module 3: Basic Data Input

- Adding an Input With Splunk Web
- Adding your Monitor Input
- Preview Data
- Specify the Source
- Select Host, Sourcetype and Index

Module 4: Managing Apps

- What is an App
- Apps configured by Default
- Viewing All Apps
- Managing Apps
- Installing an App Manually
- Enabling and Disabling Apps
- Deleting anApp
- App Permissions

Module 5: Splunk Configuration Files

- Configuration Directories
- Default vs. Local Configuration
- Global Context vs. User or App Context
- Runtime Merging of Configurations
- Configuration Testing Commands

Module 6: Universal Forwarders

- Forwarders and Indexers
- Benefits of Using Forwarders
- Splunk Universal Forwarder
- Heavy Forwarder
- Configuration Steps
- Configuring the Receiving Port
- Downloading the Universal Forwarder Installer
- Installing Universal Forwarder Manually
- Forwarder Configuration Files

Lab Setup

- ✓ RAM - >=16 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 6 virtual machines installed with Splunk software downloaded (NOT Installed) in each VM → Version : 6.5.3
  - https://www.splunk.com/en_us/download/splunk-enterprise-2.html#tabs/linux
  - https://www.splunk.com/en_us/download/universal-forwarder.html
  - 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 VMs 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, white board and marker (blue, black, green)