## 1001_M1_Splunk_Basics_Quiz

1. Which Splunk components is typically installed on the machines where data is generated?
    A. Indexer
    B. Forwarder
    C. Search Head
    D. Deployment Server

2. Which Splunk component processes raw data into events and forwards them to the indexer?
    A. Index
    B. Search Head
    C. Indexer
    D. Forwarder

3. Which Splunk component is mainly responsible for saving data to disk?
    A. Search Head
    B. Heavy Forwarder
    C. Indexer
    D. Universal Forwarder

4. What are the three basic components of Splunk?
    A. Forwarder, Indexer, Search Head
    B. Deployment Server, Indexer, Knowledge Objects
    C. Indexer, Index, Search Head
    D. Knowledge Objects, Forwarders, Indexer

5. How would you define Splunk?
    A. Database Management tool.
    B. Security Information and Event Management (SIEM).
    C. Cloud based application that helps in analyzing logs.
    D. Splunk is a software platform to search, analyze and visualize machine-generated data.

6. Which Splunk component allows users to write SPL queries to retrieve data?
    A. Forwarders
    B. Indexer

C. Heavy Forwarders
D. Search Head

7. Which Splunk component can perform log filtering and parsing?
   A. Index Forwarders
   B. Universal Forwarders
   C. Super Forwarders
   D. Heavy Forwarders

8. Which statement about user account settings and preferences is correct?
   A. Home App is the only app that can be set as the default application.
   B. Settings can only be changed by accounts with a Power User or Admin role.
   C. Time Zones are automatically updated based on the setting of the computer accessing them.
   D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

9. What do we call a collection of items such as data inputs, UI elements, and knowledge objects?
   A. An app
   B. JSON
   C. A role
   D. An enhanced solution

10. What are Splunk Apps primarily used for?
   A. Designed to cater for numerous use cases and empower Splunk.
      Allows multiple workspaces for different use cases/user roles.
      It is a collection of different Splunk config files like data inputs, UI and Knowledge Objects.
   B. Designed to cater for numerous use cases and empower Splunk.
      Allows multiple workspaces for different user cases/user roles.
      We cannot install Splunk App.
   C. We cannot install Splunk App.
      Allows multiple workspaces for different use cases/user roles.
      It is a collection of different Splunk config files like data inputs, UI and Knowledge Objects
   D. None of the above

11. Which app is included by default in Splunk Enterprise?
    A. Splunk Enterprise Security
    B. Search & Reporting
    C. Splunk Eventgen
    D. Splunk DB Connect

12. How many main user roles exist in Splunk?
    A. 2
    B. 1
    C. 4
    D. 3

13. What is the default web port number used by Splunk?
    A. 9997
    B. 8000
    C. 8089
    D. 443

14. Which three options are provided when you click the Data Summary button located just below the search bar?
    A. Indexes
    B. Hosts
    C. Sources
    D. Sourcetypes

15. What is an efficient and comprehensive method to understand the data available within a Splunk deployment?
    A. Through Splunk reports
    B. Through Splunk CLI
    C. Click Data Summary Tab in Splunk Web
    D. Search across all indexes