Splunk Enterprise – Installation, Architecture & Features (Detailed Answers)

1. Steps for Installing Splunk Enterprise on Windows

Splunk Enterprise is a powerful platform used for searching, monitoring, and analyzing machine-generated data. Below are the detailed steps to install Splunk Enterprise on a Windows operating system.

- Download Splunk Enterprise for Windows from the official Splunk website.
- Run the installer (.msi file) as Administrator.
- Accept the license agreement.
- Choose installation directory (default is recommended).
- Set administrator username and password.
- Choose whether Splunk should run as a local system user.
- Complete installation and launch Splunk.
- Access Splunk Web using http://localhost:8000 in a browser.
- Log in using admin credentials to verify installation.

2. Data Preparation and Datameer

Data Preparation: Data preparation is the process of collecting, cleaning, transforming, and organizing raw data into a usable format for analysis. It includes removing inconsistencies, handling missing values, and formatting data.

Datameer: Datameer is a big data analytics tool that runs on Hadoop. It provides an easy-to-use interface for data preparation, exploration, and visualization without requiring deep programming knowledge.

3. Functions of Search and Reporting App

- Search indexed data using SPL (Search Processing Language).
- Create real-time and historical reports.
- Generate alerts based on search results.
- Visualize data using charts and tables.
- Save and share searches and reports.
- Analyze trends and patterns in data.

4. Types of Splunk Dashboards & Components of Splunk Architecture

Types of Splunk Dashboards:

- Operational Dashboards – Monitor real-time system performance.

- Analytical Dashboards – Analyze trends and historical data.
- Executive Dashboards – Provide high-level business insights.

Components of Splunk Architecture:

- Forwarder – Collects and sends data to Splunk indexer.
- Indexer – Stores and indexes data.
- Search Head – Provides search and visualization interface.
- Deployment Server – Manages configuration updates.
- License Master – Manages Splunk licenses.

5. Benefits of Feeding Data through Splunk Forwarders

- Efficient and reliable data forwarding.
- Minimal resource usage on source machines.
- Secure data transmission using encryption.
- Scalable data collection across large environments.
- Centralized management of data inputs.
- Supports load balancing and failover.