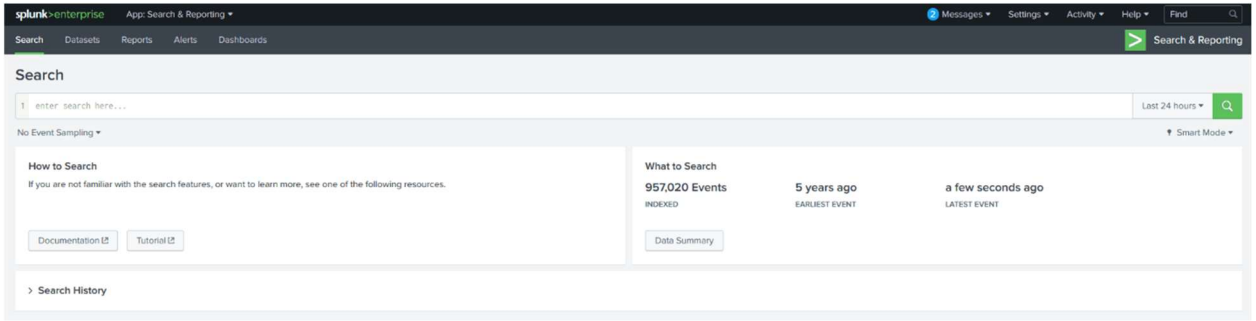
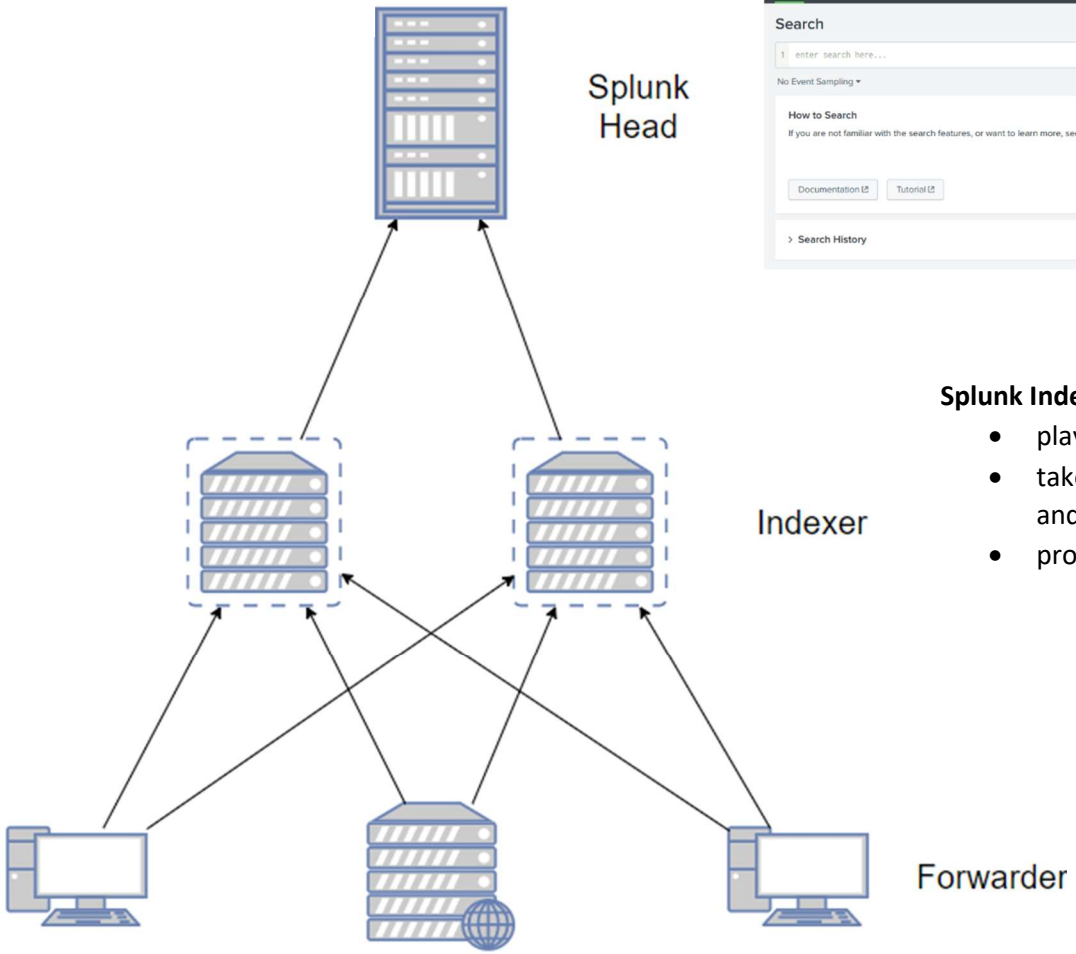
Search Head

- place within the Search & Reporting App where users can search the indexed





Splunk Indexer

- plays the main role in processing the data it receives from forwarders
- takes the data, normalizes it into the field value pairs, determines the data type, and stores them as events
- processed data is then easy to search and analyse

Splunk Forwarder

- lightweight agent installed on the endpoint intended to be monitored
- main task is to collect the data and send it to the Splunk instance
- does not affect endpoint performance as it takes very few resources to process

Examples of key data sources:

- Web server generating web traffic
- Windows machine generating Windows Event Logs, PowerShell, and Sysmon data
- Linux host generating host centric logs
- database generating DB connection requests, responses, and errors