

Ingest Data 🡪 Index Data 🡪 Visualize Data

**Splunk Terms:**

Index –

Events – A single row in a table

Search –

Pivot – Any kind of Visualization

Dashboard – Collection of Pivots

Forwarder – Script which is used to send data to Splunk db

**Setting up the Splunk environment**

Splunk Licensing – This is free upto 500 MB/per day usage. Three different Splunk flavours are enterprise, cloud, light

<http://localhost:8000/en-US/account/logout>

rajee/password

Splunk uses Splunk Processing Language(SPL)

**Splunk Search Commands**

host="DESKTOP-S1LD48L" | dedup sourcetype // Removes duplicates on source type

host="DESKTOP-S1LD48L" | search EventCode=100 | search SourceName=Bonjour\*

host="DESKTOP-S1LD48L" | head 10

host="DESKTOP-S1LD48L" | tail 10

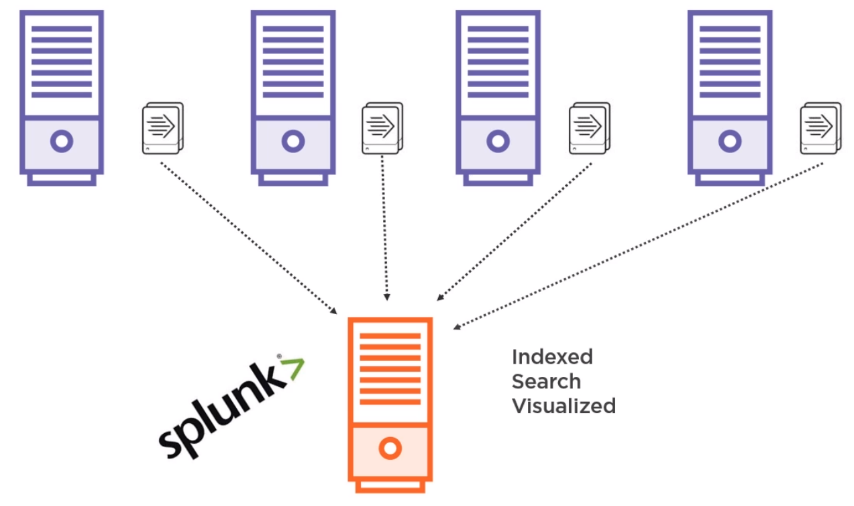
host="DESKTOP-S1LD48L" | top 10 EventCode

Local data can be stored as alerts or report

**Enterprise Splunk Architecture**

**Forwarder :** This is like an agent that is installed on the remote machine to forward the data to another machine. In short, it is an instance of splunk that sends data to another instance of splunk





**Application Development in Splunkbase**

Splunkbase : Place to create apps or use existing apps so that we can get data from those apps and do the analysis using Splunk.

<https://splunkbase.splunk.com/>

