8089

8089

**9997**

Splunk Indexer

IndexA / IndexB / IndexC

**Splunk Forwarder Agent**

**Inputs –What to send**

**Outputs – Whom to send**

Application Server

Log1 / Log2 / Log3

**Steps to follow**

* Choose Application server and have some logs to monitor
* Install Splunk Universal forwarder (UF) in Application server – Splunk Installation with forwarder package ( splunkforwarder)

Refer Installation Doc

* Configure Input and Output in UF agent to send data to Indexer
* Take One instance and install Splunk Full Package to make it as Indexer - Splunk Installation with Full package
* Web is available for Indexer. Go to web and enable the receiving port – Refer Indexer Conf doc
* Then you will be able to collect the data from forwarder to indexer

Check:

Go to Indexer web then search with your index “index=student” (By default it is going to store in main index)

**Input**:

Create a monitor stanza : Specify path of file what you want to read ; Specify where you are going to store in indexer ( so many indexes are there)

**Output**

Create a tcpout stanza : Specify your indexer ip address and receiving port

Note: After editing/creating any conf file you have to restart the splunk service