SPLUNK INSTALLATION

Master splunk enterprise

Cd /opt

wget -O splunk-8.2.6-a6fe1ee8894b-Linux-x86\_64.tgz <https://download.splunk.com/products/splunk/releases/8.2.6/linux/splunk-8.2.6-a6fe1ee8894b-Linux-x86_64.tgz>

cd splunk/bin

./splunk start

<http://ip:8000> 🡪 in browser

Slave

Cd /opt

wget -O splunkforwarder-8.2.6-a6fe1ee8894b-Linux-x86\_64.tgz "https://download.splunk.com/products/universalforwarder/releases/8.2.6/linux/splunkforwarder-8.2.6-a6fe1ee8894b-Linux-x86\_64.tgz"cd splunk/bin

./splunk start

Components of splunk

1.Search head

2.Indexers

3.forwaders

Configuration

MASTER

Master listener port 9997

Step:1 ./splunk enable listen 9997

SLAVE

./splunk add forward-server 3.94.153.93:9997

Add syslog file to slave using winscp and move to /var/log

./splunk add monitor /var/log/syslog –index main

Then go to ui and type in search index=”main”

How to write a query in splunk

We write index with hostname and source which is path and source type which is file name