**Splunk**

Note: port 8000 for apache and 8089 for management

Download with wget

wget -O splunk-6.3.2-aaff59bb082c-Linux-i686.tgz '<http://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86&platform=linux&version=6.3.2&product=splunk&filename=splunk-6.3.2-aaff59bb082c-Linux-i686.tgz&wget=true>'

tar -xvpf

cp -R splunk /opt/splunk

cd /opt/splunk/bin

./splunk start --accept-licence

**REDHAT**

**echo "Installing SPLUNK server"**

echo "USER SPLUNK SHOULD ALREADY EXIST"

# Testing on Redhat 7

# I have to extract and then copy the folder because some distros do not have the -C commmand

tar -xzvf ./include/raw/release/splunk6\_64.tgz

cp -Rp ./splunk /opt/splunk

chown -R splunk:splunk /opt/splunk

chmod -R 755 /opt/splunk

/opt/splunk/bin/./splunk start --accept-license

/opt/splunk/bin/./splunk enable boot-start -user splunk

**echo "Installing forwarder"**

echo "USER SPLUNK SHOULD ALREADY EXIST"

# Testing on Redhat 7

# I have to extract and then copy the folder because some distros do not have the -C commmand

tar -xzvf ./include/raw/release/splunkforwarder5\_64.tgz

cp -Rp ./splunkforwarder /opt/splunkforwarder

chown -R splunk:splunk /opt/splunkforwarder

chmod -R 755 /opt/splunkforwarder

/opt/splunkforwarder/bin/./splunk start --accept-license

/opt/splunkforwarder/bin/./splunk enable boot-start -user splunk

echo "First Type in full Host name of Splunk central server (example 192.168.0.1 OR domain.site2.whatever) "

su - splunk -c " whoami;

cd /opt/splunkforwarder/bin;

./splunk add forward-server $\_SHOST:$\_SPORT;

./splunk add monitor /var/log;

./splunk restart;

whoami "