Splunk forwarder setup.

* Can download the forwarder from <https://www.splunk.com/en_us/download/universal-forwarder/thank-you-universalforwarder.html>
* wget -O splunkforwarder-7.2.1-be11b2c46e23-linux-2.6-amd64.deb 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86\_64&platform=linux&version=7.2.1&product=universalforwarder&filename=splunkforwarder-7.2.1-be11b2c46e23-linux-2.6-amd64.deb&wget=true'

sudo dpkg -I <splunk .deb file>

splunk installs with the user splunk. Reset the password sudo passwd splunk

once password is reset, go to /opt/splunkforwarder/bin

switch users to the splunk user.

run ./splunk start –accept-license

it will have you then create your splunk admin username and password.

splunk: splunkadmin

switch to the sudo user

run sudo ./splunk enable boot-start

sudo su splunk

run ./splunk set deploy-poll 192.168.1.14:9998

* the ip above is the ip that I have the box the forwarder is being installed on set to and the port we will be using

run ./splunk add forward-server 192.168.1.13:9998 -auth splunkadmin:password

* this is the actual splunk hosts ip and receiving port

run ./splunk list forward-server

* this will tell us if there is an active forward going to the box or not. If it is active or only configured and inactive

go to /opt/splunkforwarder/etc/system/local.

Edit the inputs.conf file and add [monitor:///your/log/location/here/\*]

Restart splunk /opt/splunkforwarder/bin ./splunk restart

<http://docs.splunk.com/Documentation/Splunk/6.2.3/Forwarding/Deployanixdfmanually>

forward server inactive: <https://answers.splunk.com/answers/48760/how-to-activate-forward-server.html>

firewall d enable/start: <https://www.liquidweb.com/kb/how-to-start-and-enable-firewalld-on-centos-7/>

firewall-cmd to add/list ports: <https://www.rootusers.com/how-to-open-a-port-in-centos-7-with-firewalld/>