Installing splunk on centos7

Follow this doc for installing <https://linoxide.com/monitoring-2/install-splunk-centos-7/>

sudo yum install wget

wget -O splunk-7.2.1-be11b2c46e23-Linux-x86\_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86\_64&platform=linux&version=7.2.1&product=splunk&filename=splunk-7.2.1-be11b2c46e23-Linux-x86\_64.tgz&wget=true'

once installed

sudo ./splunk start –accept-license

<https://ddewaele.github.io/networking/ssh/changing-the-ssh-port/>

https://linuxize.com/post/how-to-install-iptables-on-centos-7/

1. check the port and hostname are right, sometime hostname may not be resolved so use the IP address  
   ./splunk show web-port
2. check startwebserver =1  
   ./splunk cmd btool web list --debug |grep startwebserver
3. Run these commands to open the iptables/ports in Unix machines  
   sudo firewall-cmd --zone=public --add-port=8000/tcp --permanent  
   sudo firewall-cmd –reload

Set up iptables on centos

# Firewall configuration written by system-config-firewall

 # Manual customization of this file is not recommended.

 \*filter :INPUT DROP [0:0] :OUTPUT DROP [0:0] :FORWARD DROP [0:0]

 # Open port for ping

 -A INPUT -p icmp -j ACCEPT

 # Open port for SSH

 -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

 -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

 # Open port for https (Splunk website)

 -A INPUT -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT

 -A OUTPUT -o eth0 -p tcp --sport 443 -m state --state NEW,ESTABLISHED -j ACCEPT

 # Open port for splunkd services

 -A INPUT -i eth0 -p tcp --dport 8089 -m state --state NEW,ESTABLISHED -j ACCEPT

 -A OUTPUT -o eth0 -p tcp --sport 8089 -m state --state NEW,ESTABLISHED -j ACCEPT

 # Open port for Splunk Forwarders

 -A INPUT -i eth0 -p tcp --dport 9997 -m state --state NEW,ESTABLISHED -j ACCEPT

 -A OUTPUT -o eth0 -p tcp --sport 9997 -m state --state NEW,ESTABLISHED -j ACCEPT

```