Splunk installation:

🡪Create ec2-instance and login to ec2-user

🡪login to splunk and download splunk enterprise edition and download linux rpm package and copy rpm package from windows to our ec2-server.

[www.splunk.com/login](http://www.splunk.com/login)

download splunk in local system and copy it using filezilla

🡪install splunk

Rpm -I splunk package

🡪go to start splunk

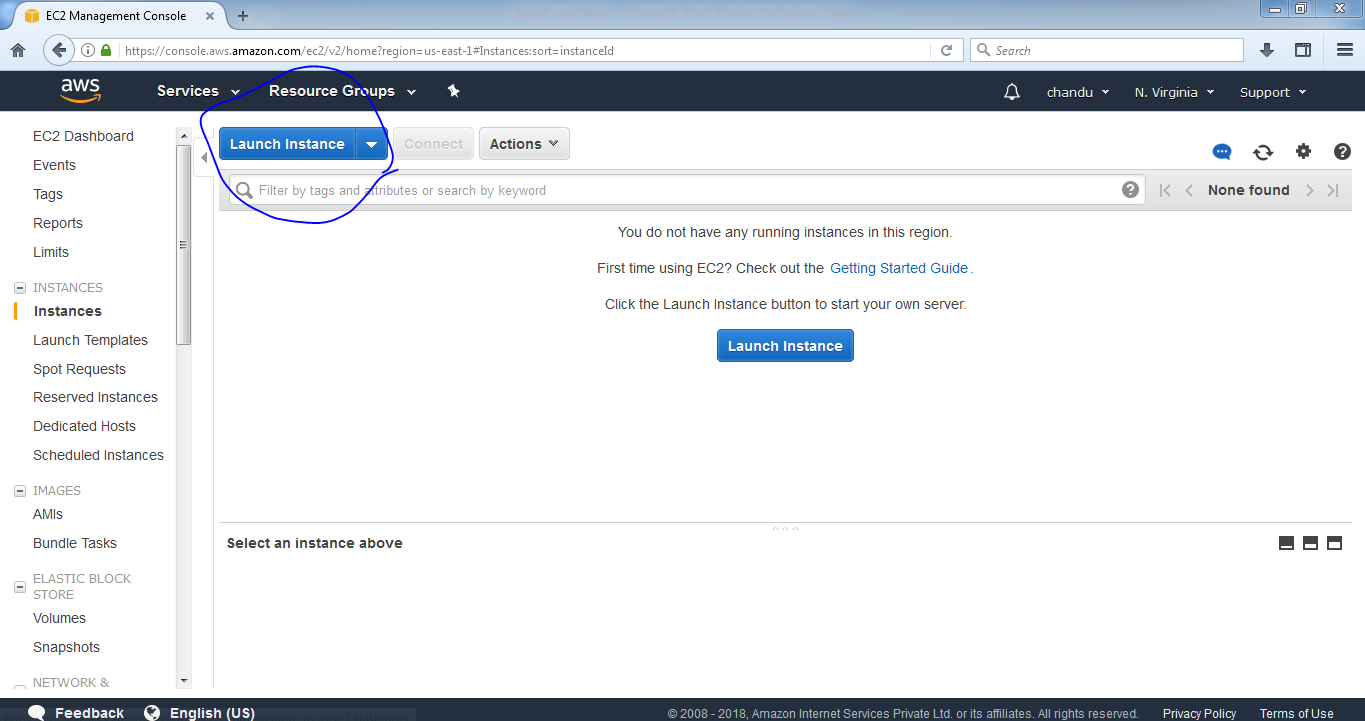
Cd /opt 🡪 Cd splunk 🡪 Cd bin 🡪./splunk start and ./splunk stop

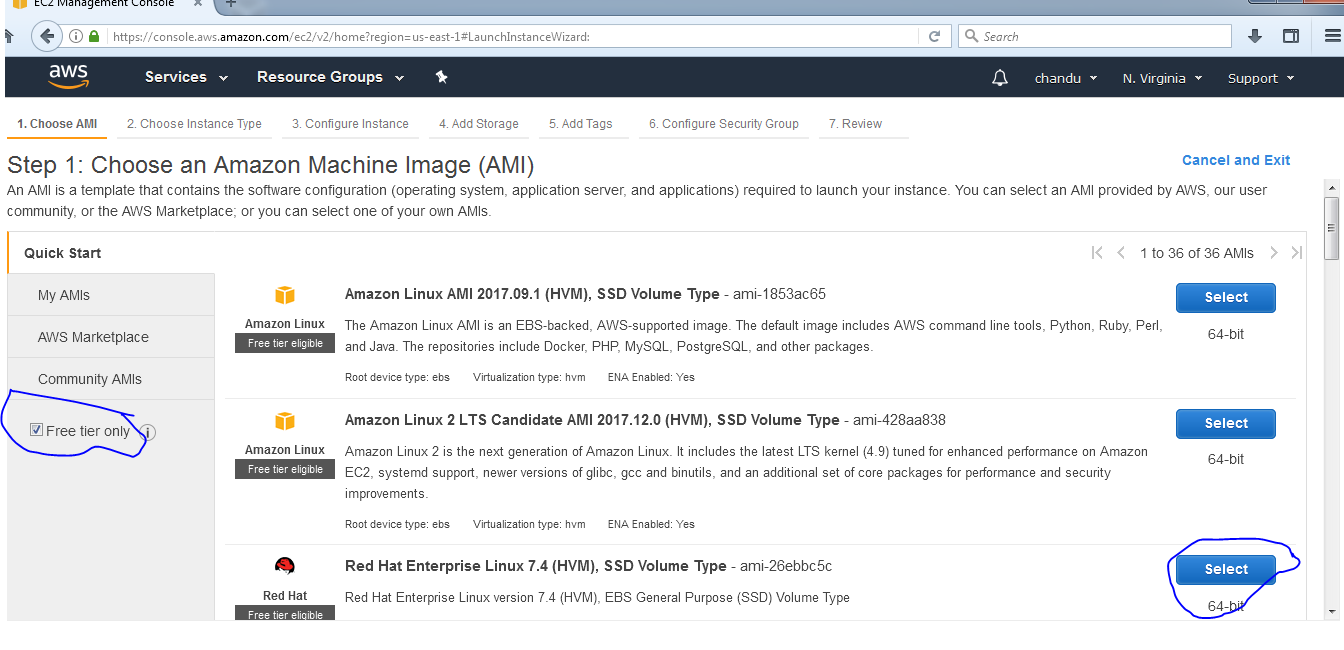
🡪now splunk started and check in browser with hostname:8000

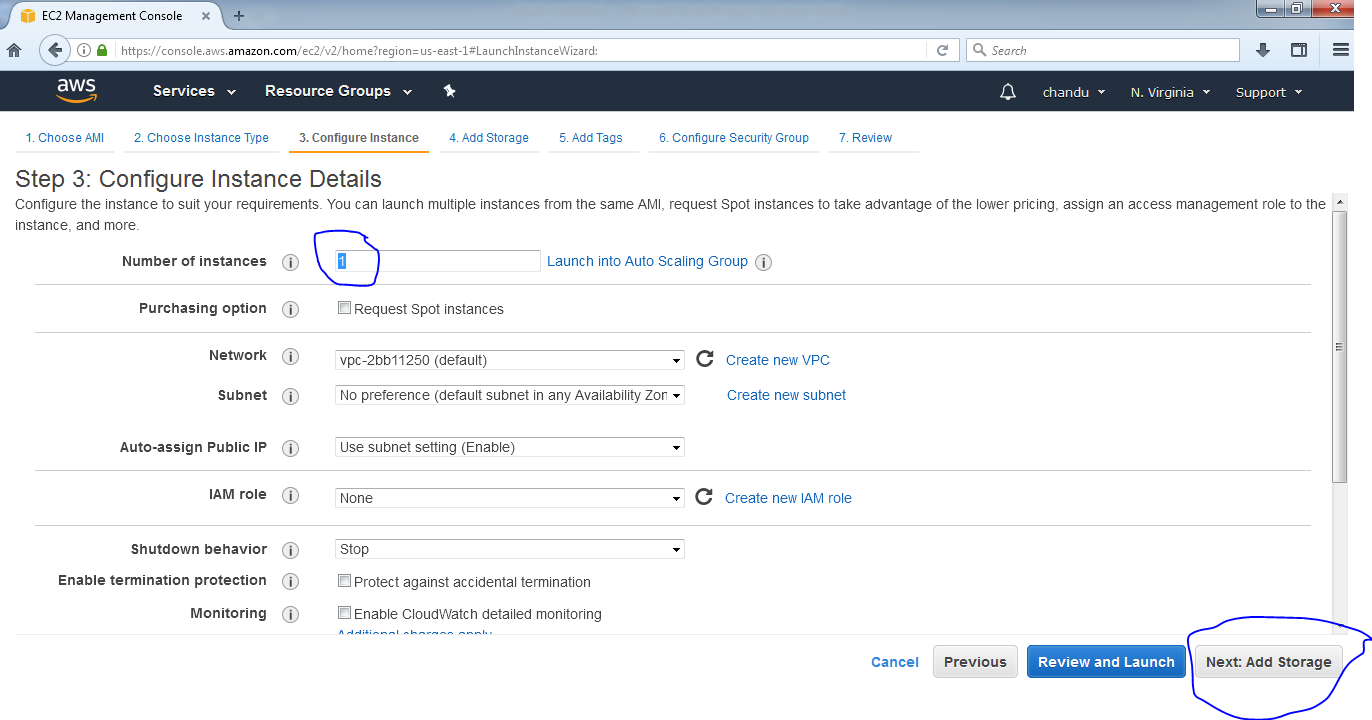
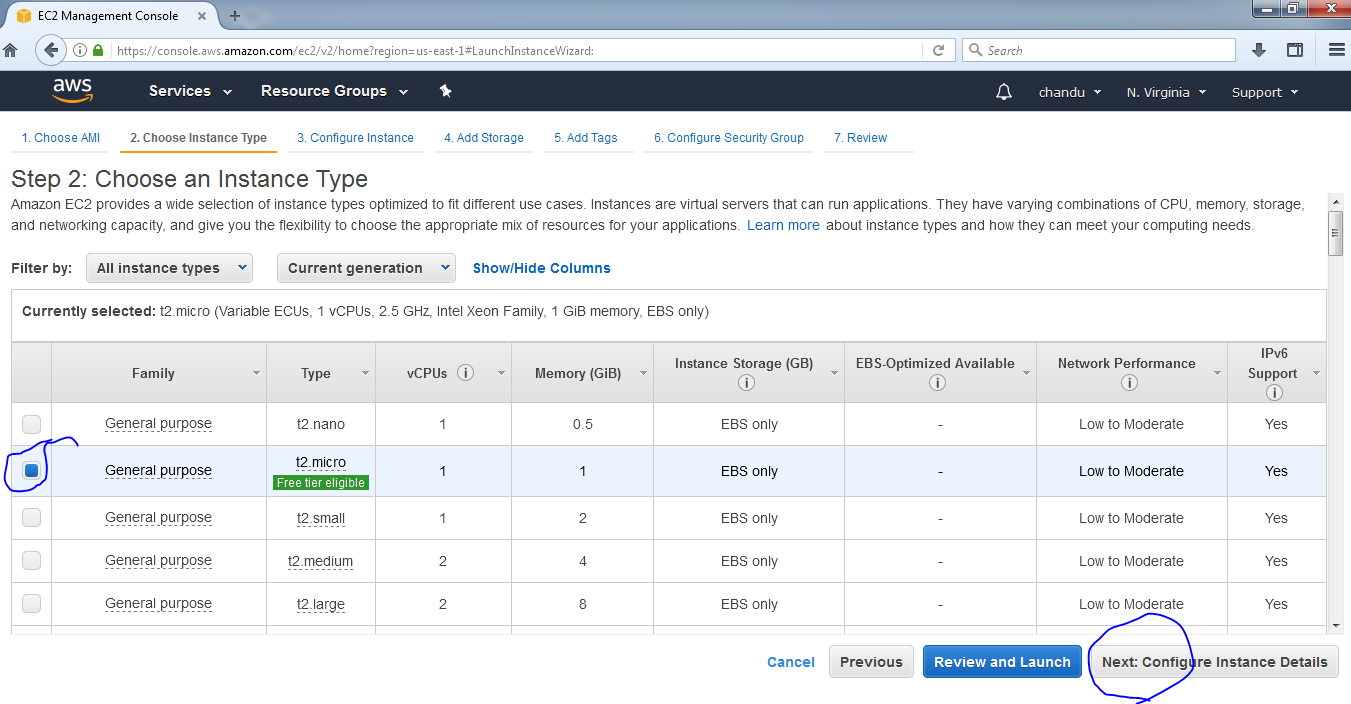
Publicip:8000

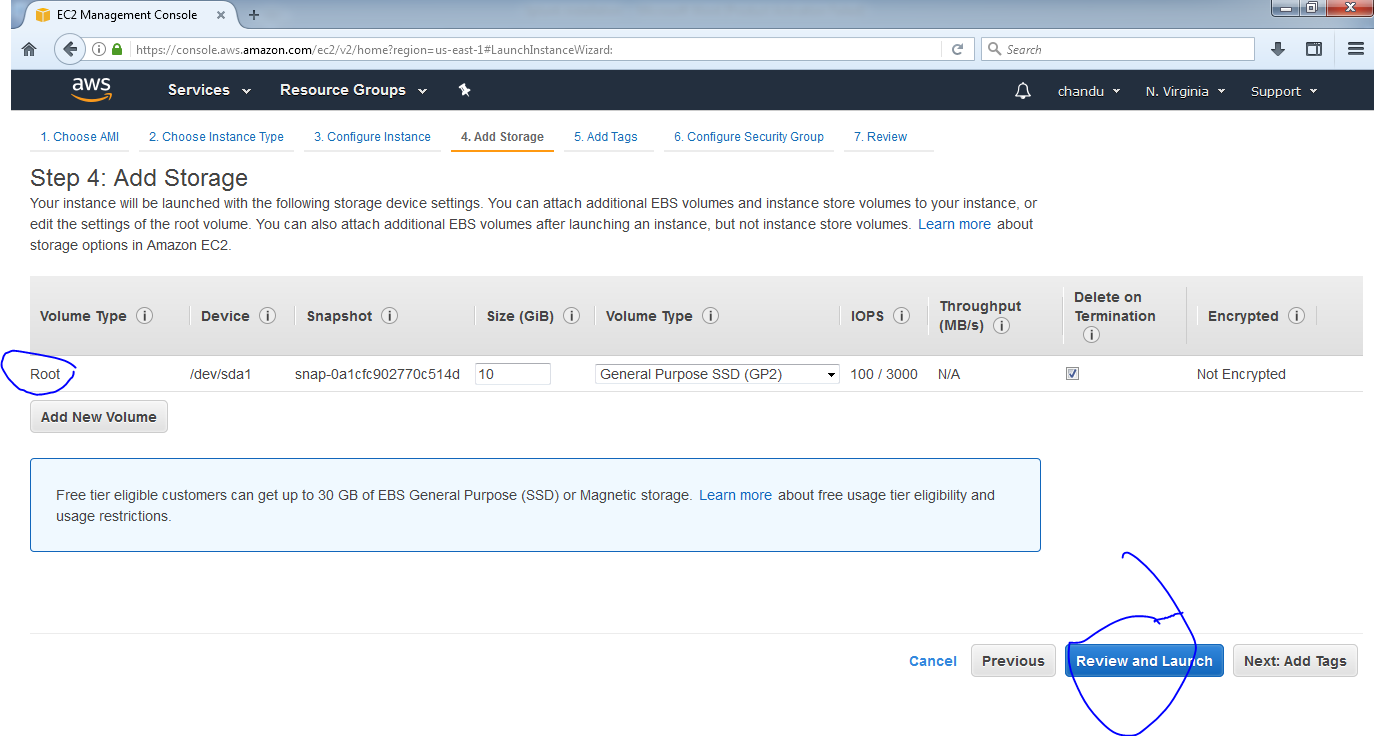
CREATE EC2-instance REDHAT LINUX

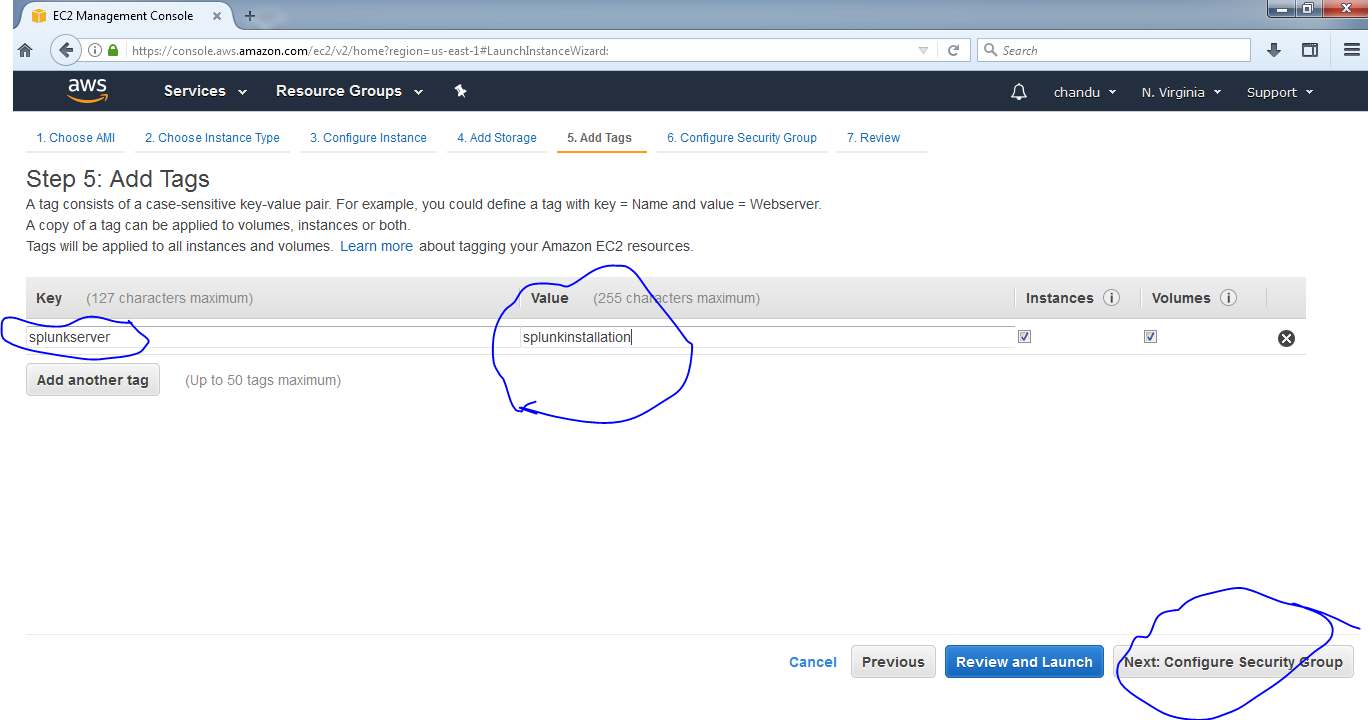
Launch instance

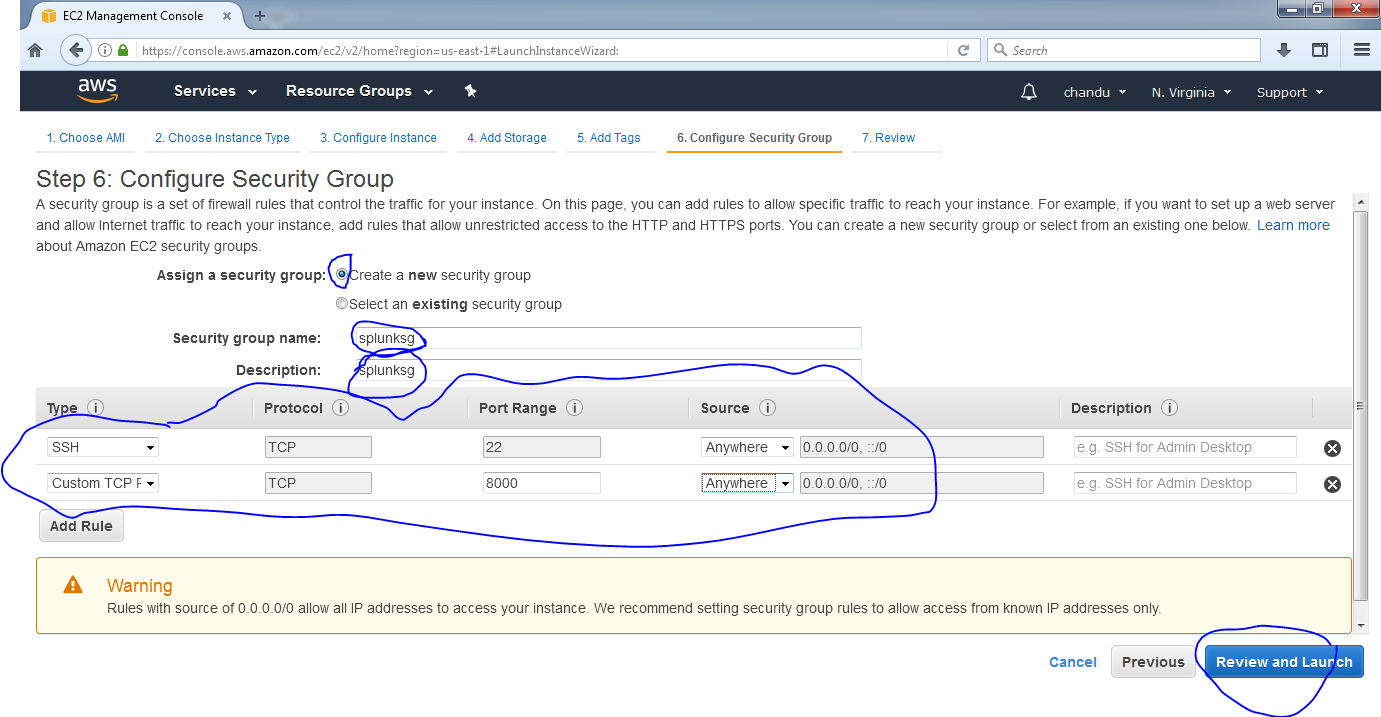


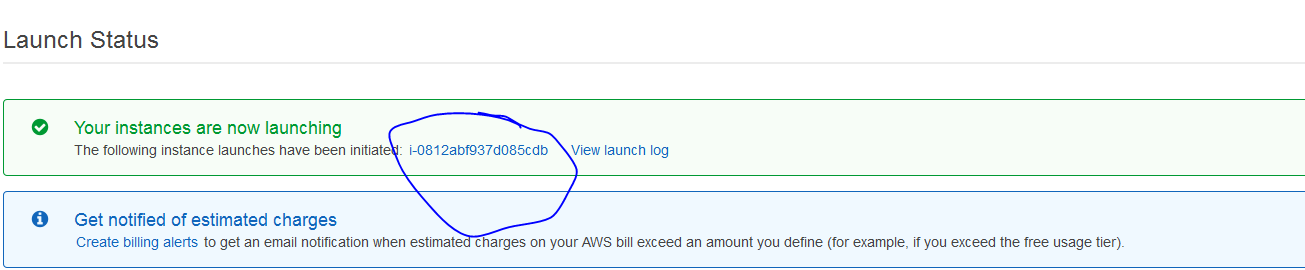
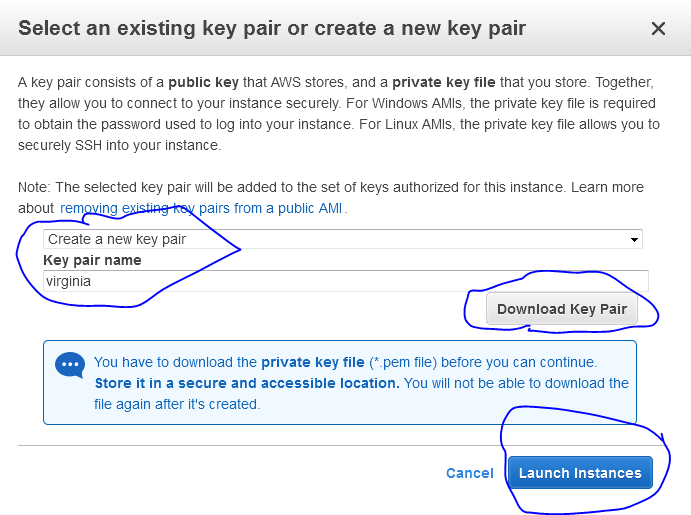
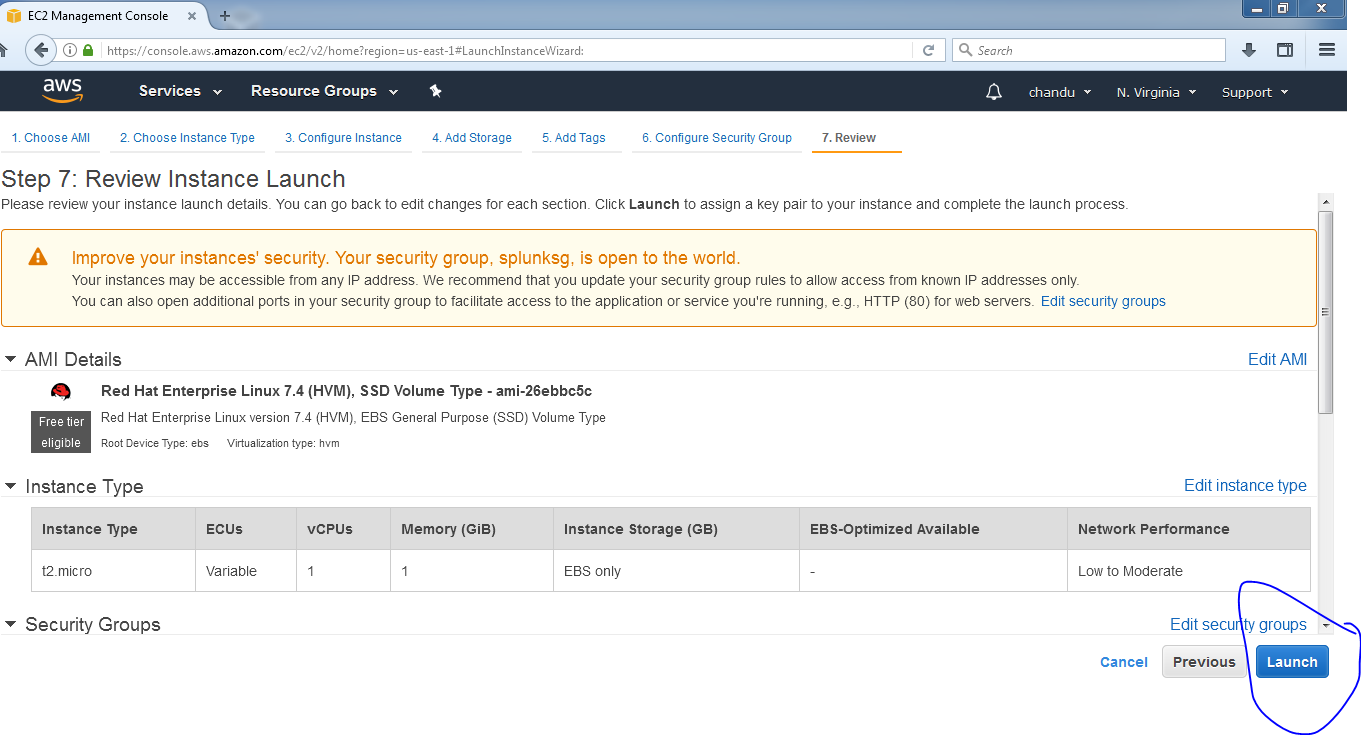




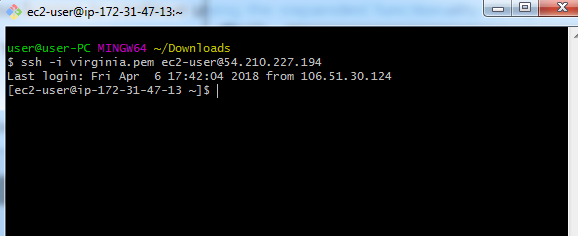




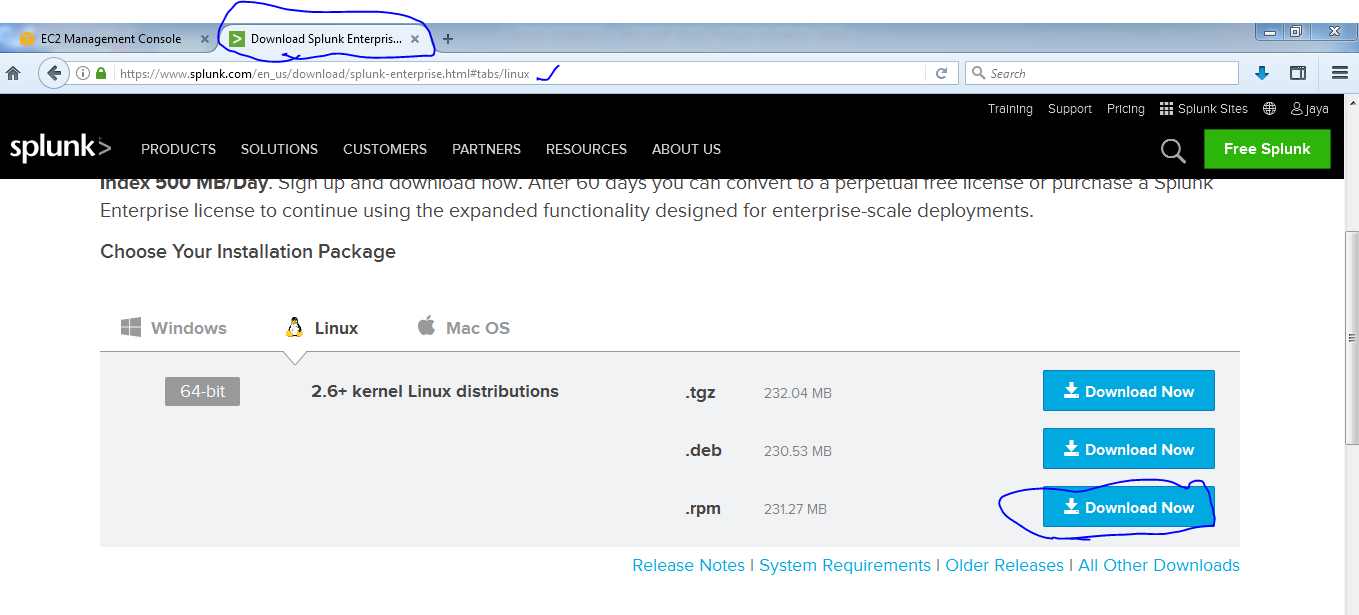


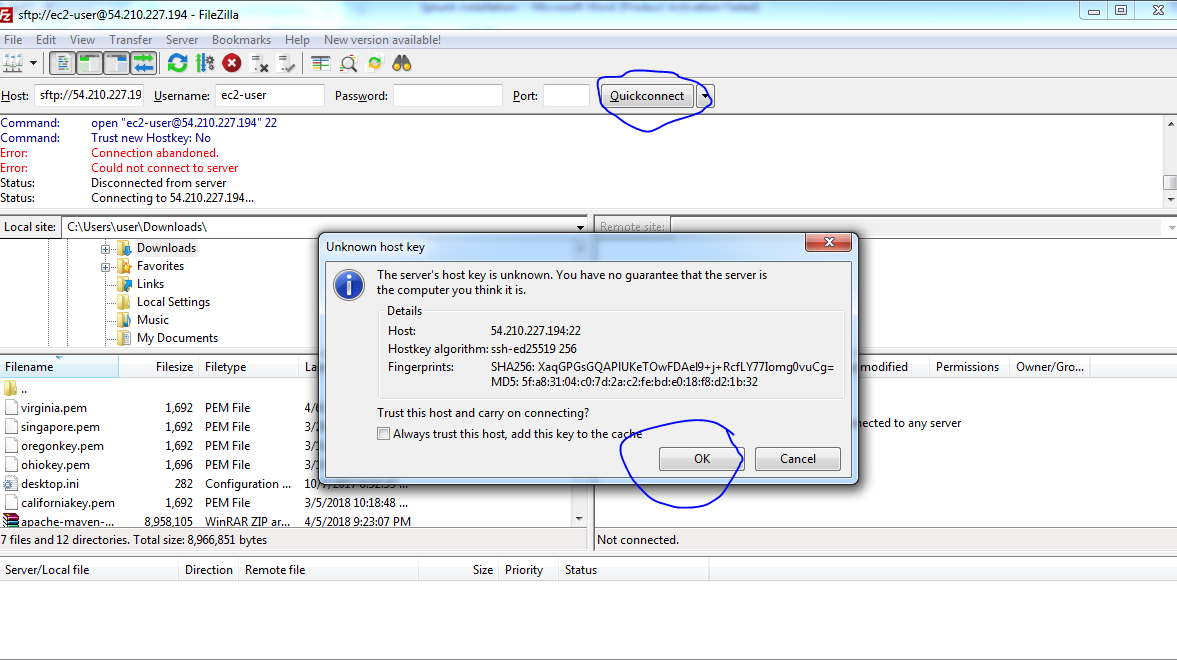
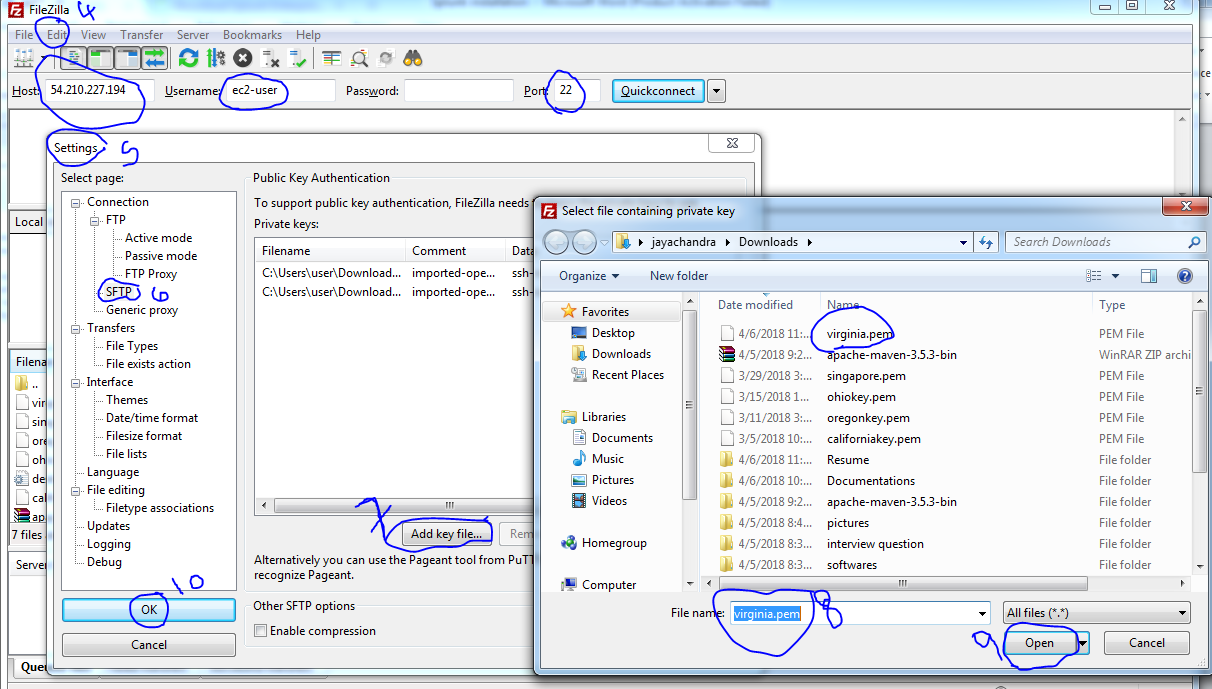


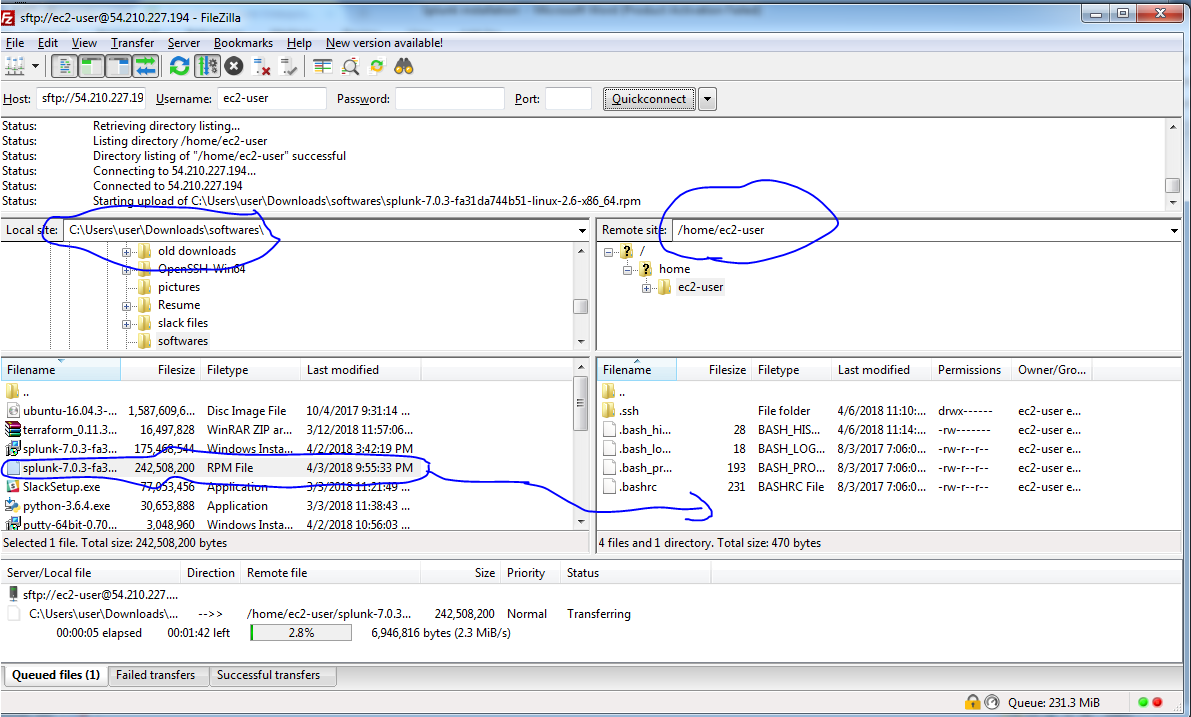
**Connect to ec2 by using gitbash or putty**



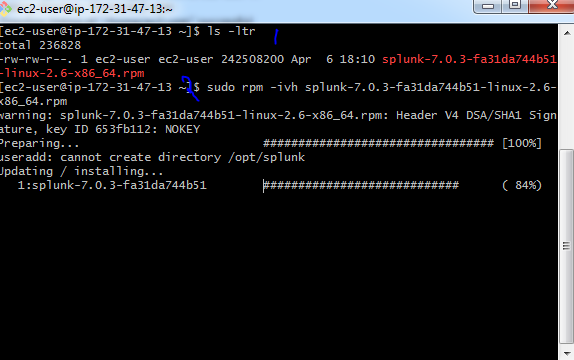
**Now download splunk for linux in windows server and copy it to linux server using filezilla**







**Now go and check in splunkserver**



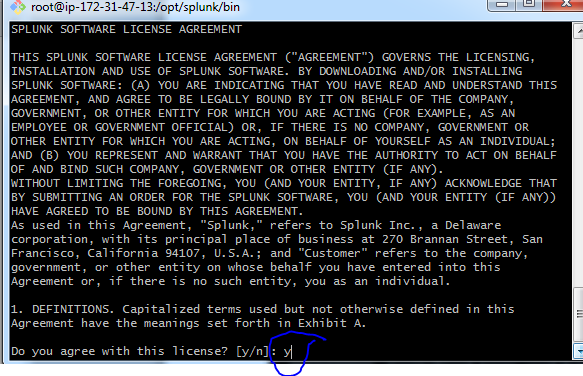
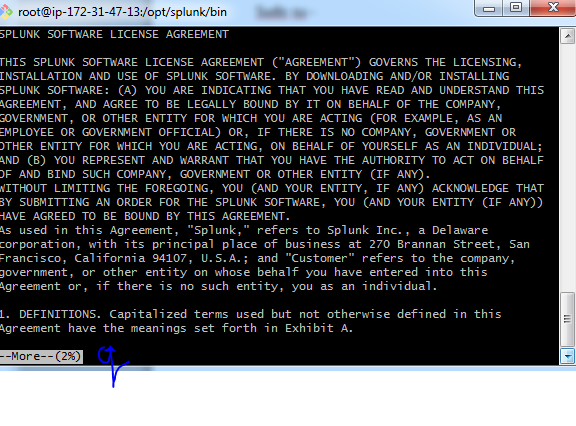
Now default splunk installed in /opt directory

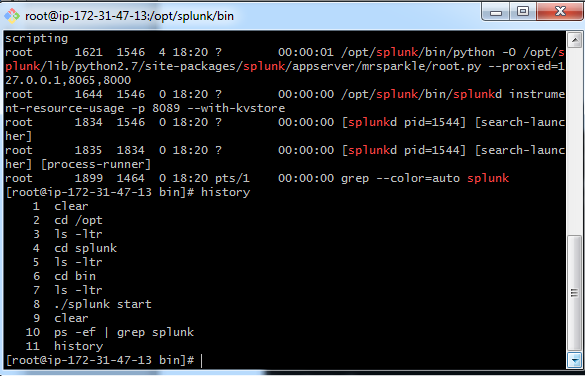
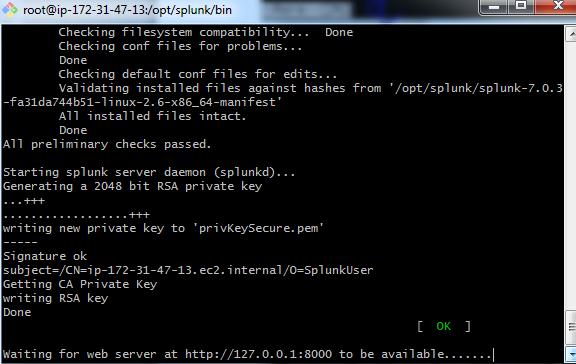
Sudo su -

Cd /opt/splunk/bin

Start splunk 🡪 ./splunk start

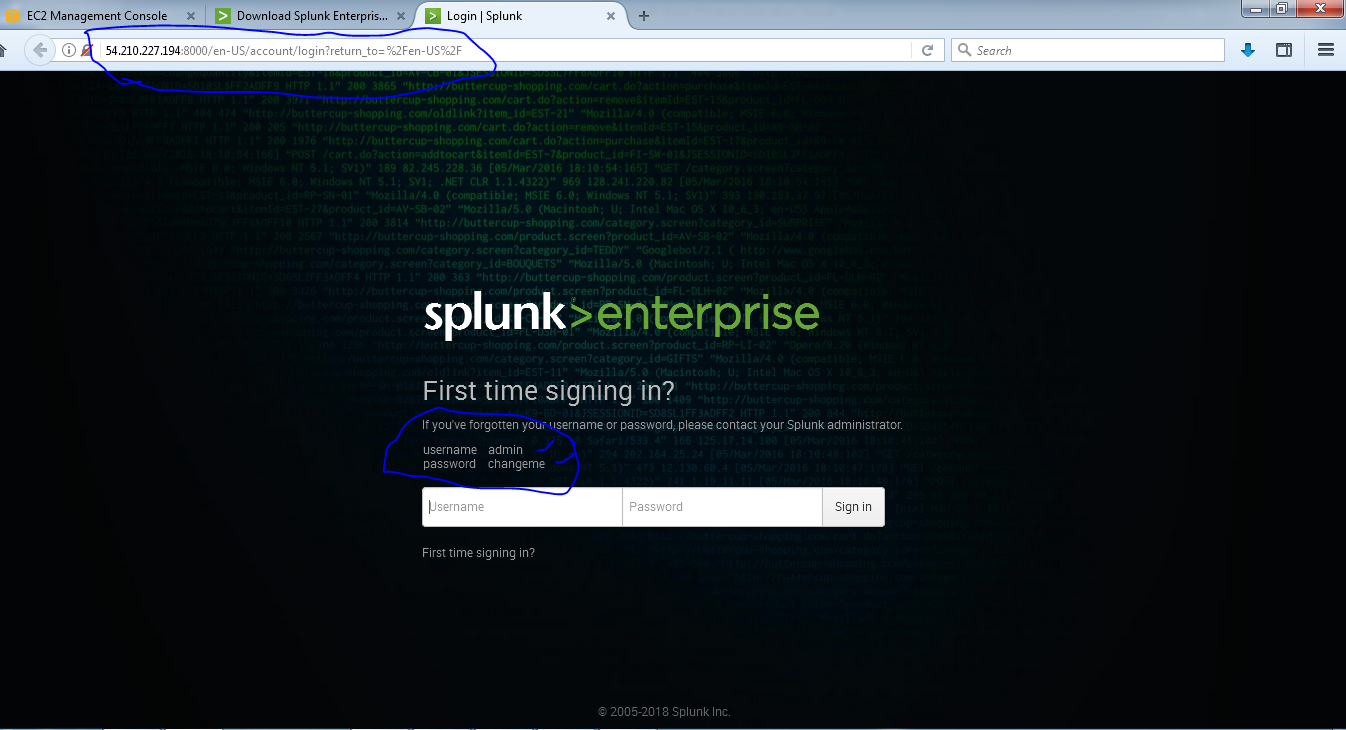
Quit enter q and y

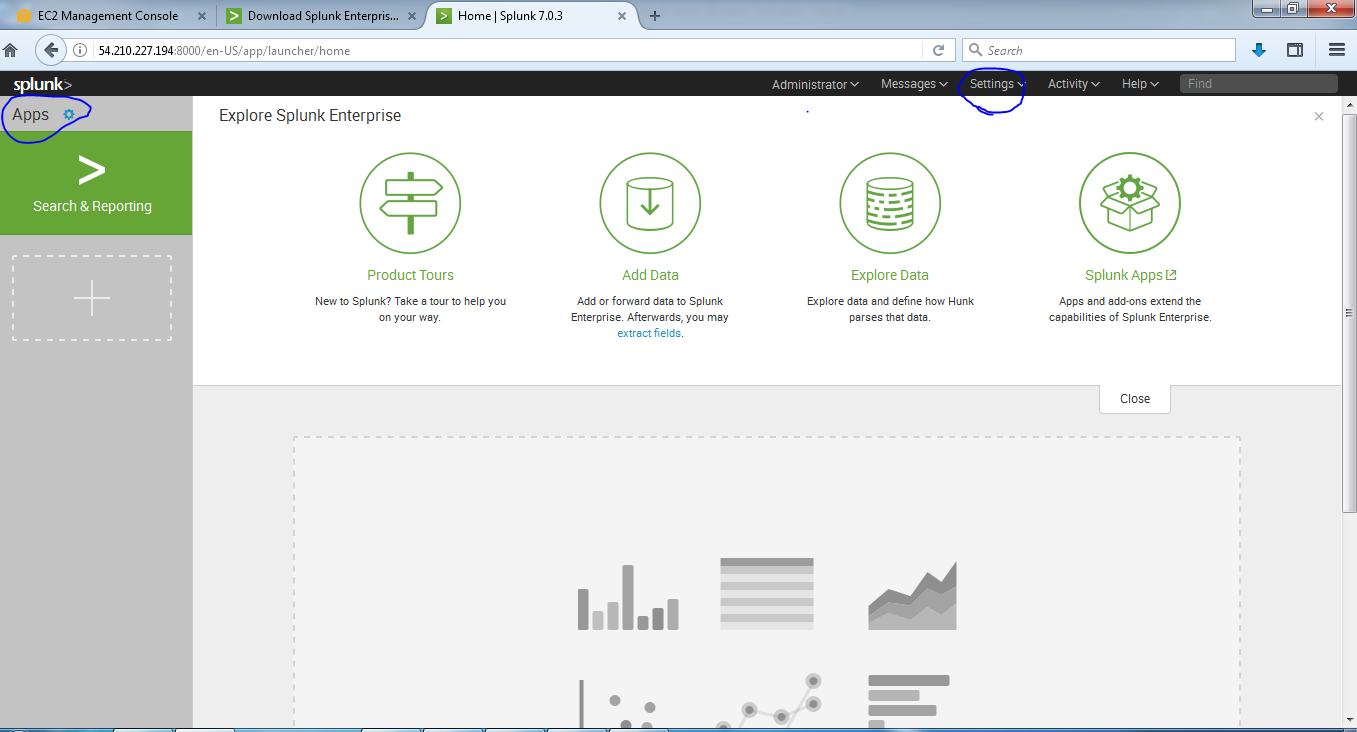




Now take public ip and browser with port 8000

Publicip:8000





This is splunk monitoring page