Splunk Installation Guide for LINUX

Installation Guide

edureka!

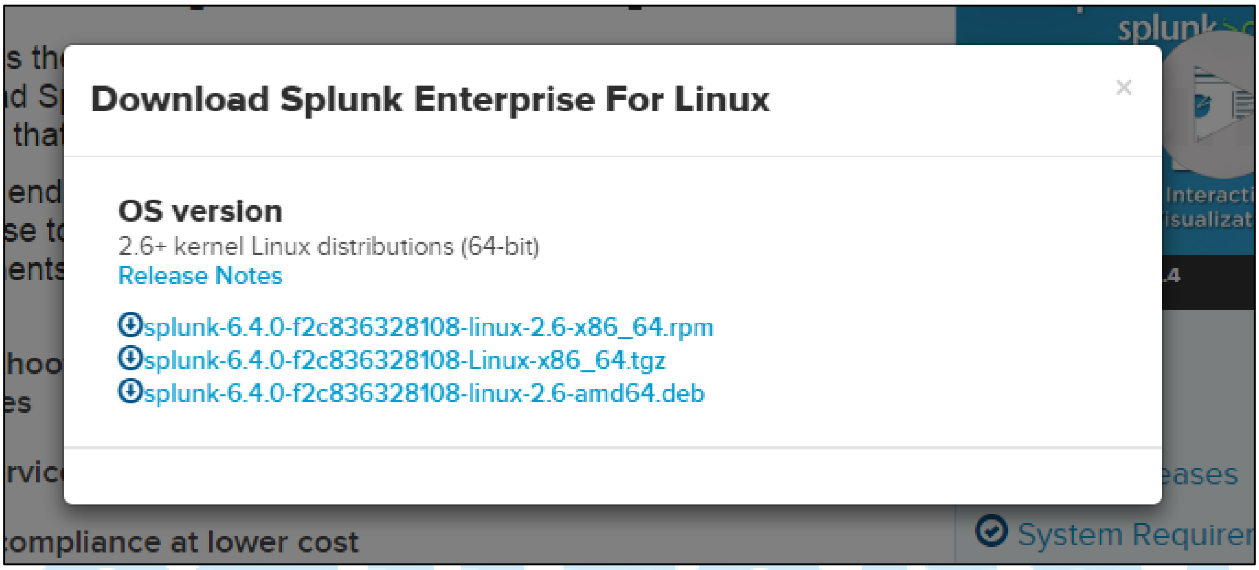
Version 1.0

Splunk Installation Guide for LINUX

Go to this link and download the splunk tool:
https://www.splunk.com/en_us/download/splunk-enterprise.html

Pre-requisite: You must have a 64-bit Linux OS to install Splunk in your machine.

From the link provided earlier, choose to download the .tgz file, which is a Tar file.



Download Splunk Enterprise For Linux

OS version

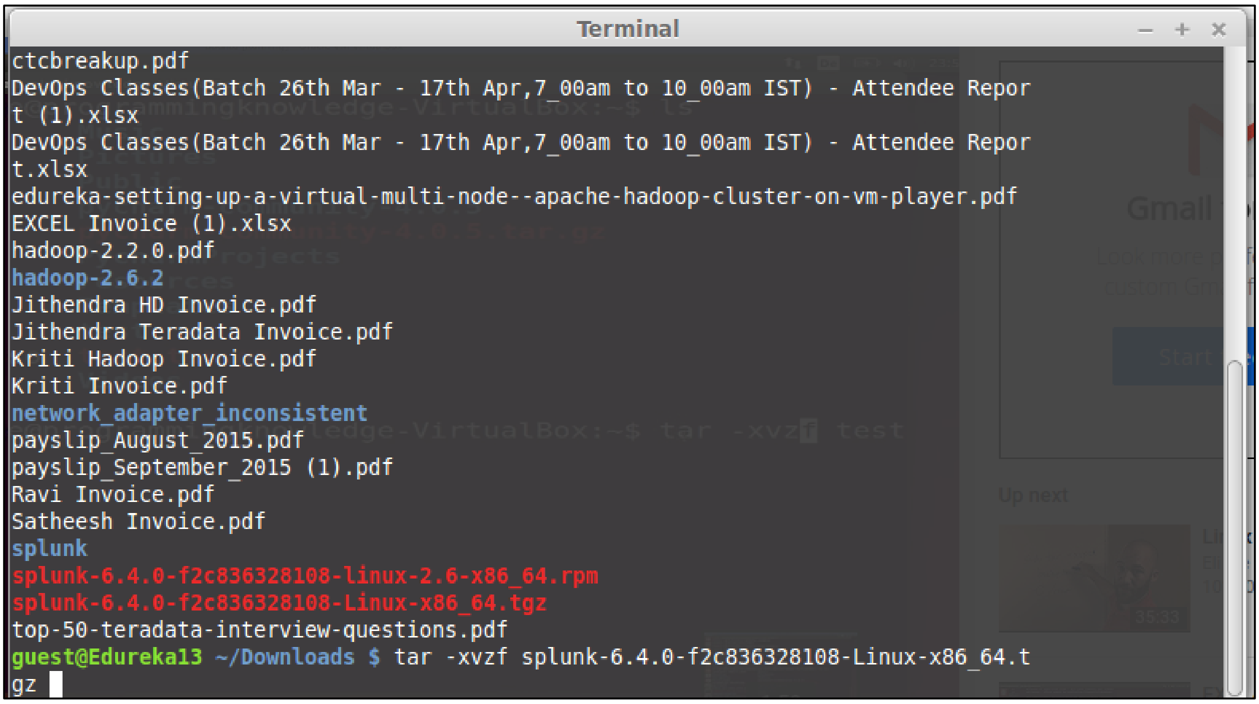
2.6+ kernel Linux distributions (64-bit)

Release Notes

splunk-6.4.0-f2c836328108-linux-2.6-x86_64.rpm
splunk-6.4.0-f2c836328108-Linux-x86_64.tgz
splunk-6.4.0-f2c836328108-linux-2.6-amd64.deb

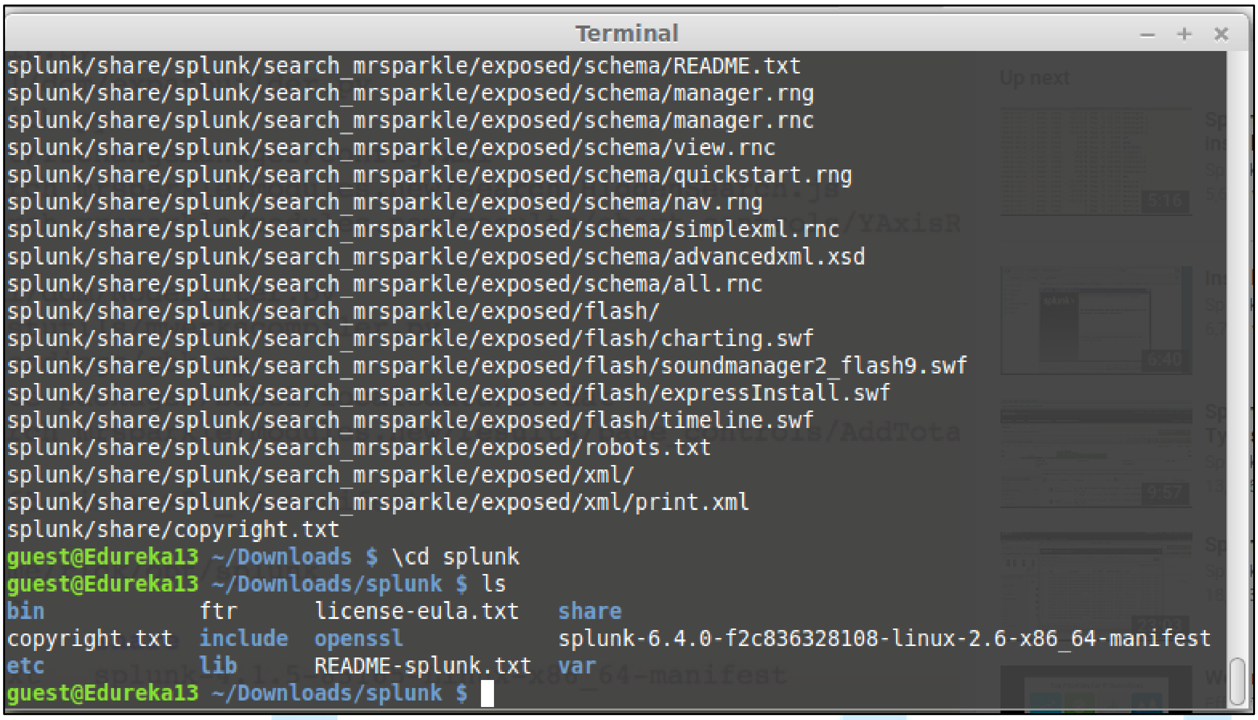
Now from the terminal, we run the following command to extract the Tar file:

tar –xvzf 'filename.tgz'



```
ctcbreakup.pdf
DevOps Classes(Batch 26th Mar - 17th Apr,7_00am to 10_00am IST) - Attendee Repor
t (1).xlsx
DevOps Classes(Batch 26th Mar - 17th Apr,7_00am to 10_00am IST) - Attendee Repor
t.xlsx
edureka-setting-up-a-virtual-multi-node--apache-hadoop-cluster-on-vm-player.pdf
EXCEL Invoice (1).xlsx
hadoop-2.2.0.pdf
hadoop-2.6.2
Jithendra HD Invoice.pdf
Jithendra Teradata Invoice.pdf
Kriti Hadoop Invoice.pdf
Kriti Invoice.pdf
network_adapter_inconsistent
payslip_August_2015.pdf
payslip_September_2015 (1).pdf
Ravi Invoice.pdf
Satheesh Invoice.pdf
splunk
splunk-6.4.0-f2c836328108-linux-2.6-x86_64.rpm
splunk-6.4.0-f2c836328108-Linux-x86_64.tgz
top-50-teradata-interview-questions.pdf
guest@Edureka13 ~/Downloads $ tar -xvzf splunk-6.4.0-f2c836328108-Linux-x86_64.t
gz
```

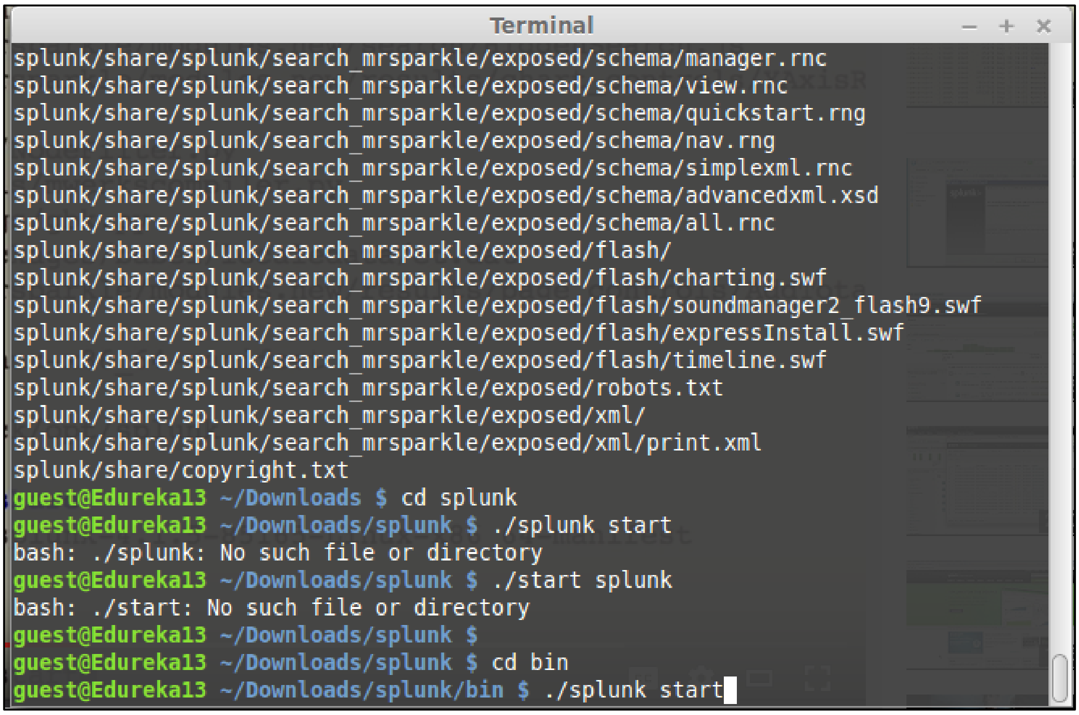
The following contents will be extracted:



```
splunk/share/splunk/search_mrsparkle/exposed/schema/README.txt
splunk/share/splunk/search_mrsparkle/exposed/schema/manager.rng
splunk/share/splunk/search_mrsparkle/exposed/schema/manager.rnc
splunk/share/splunk/search_mrsparkle/exposed/schema/view.rnc
splunk/share/splunk/search_mrsparkle/exposed/schema/quickstart.rng
splunk/share/splunk/search_mrsparkle/exposed/schema/nav.rng
splunk/share/splunk/search_mrsparkle/exposed/schema/simplexml.rnc
splunk/share/splunk/search_mrsparkle/exposed/schema/advancedxml.xsd
splunk/share/splunk/search_mrsparkle/exposed/schema/all.rnc
splunk/share/splunk/search_mrsparkle/exposed/flash/
splunk/share/splunk/search_mrsparkle/exposed/flash/charting.swf
splunk/share/splunk/search_mrsparkle/exposed/flash/soundmanager2_flash9.swf
splunk/share/splunk/search_mrsparkle/exposed/flash/expressInstall.swf
splunk/share/splunk/search_mrsparkle/exposed/flash/timeline.swf
splunk/share/splunk/search_mrsparkle/exposed/robots.txt
splunk/share/splunk/search_mrsparkle/exposed/xml/
splunk/share/splunk/search_mrsparkle/exposed/xml/print.xml
splunk/share/copyright.txt
guest@Edureka13 ~/Downloads $ \cd splunk
guest@Edureka13 ~/Downloads/splunk $ ls
bin            ftr      license-eula.txt   share
copyright.txt  include  openssl            splunk-6.4.0-f2c836328108-linux-2.6-x86_64-manifest
etc            lib      README-splunk.txt  var
guest@Edureka13 ~/Downloads/splunk $ 
```

The files would have been extracted under a new Directory called splunk. We should use the command cd splunk to enter that directory and then again use cd bin to enter the bin directory.

We can start the Splnuk service now by giving the command ./splunk start.

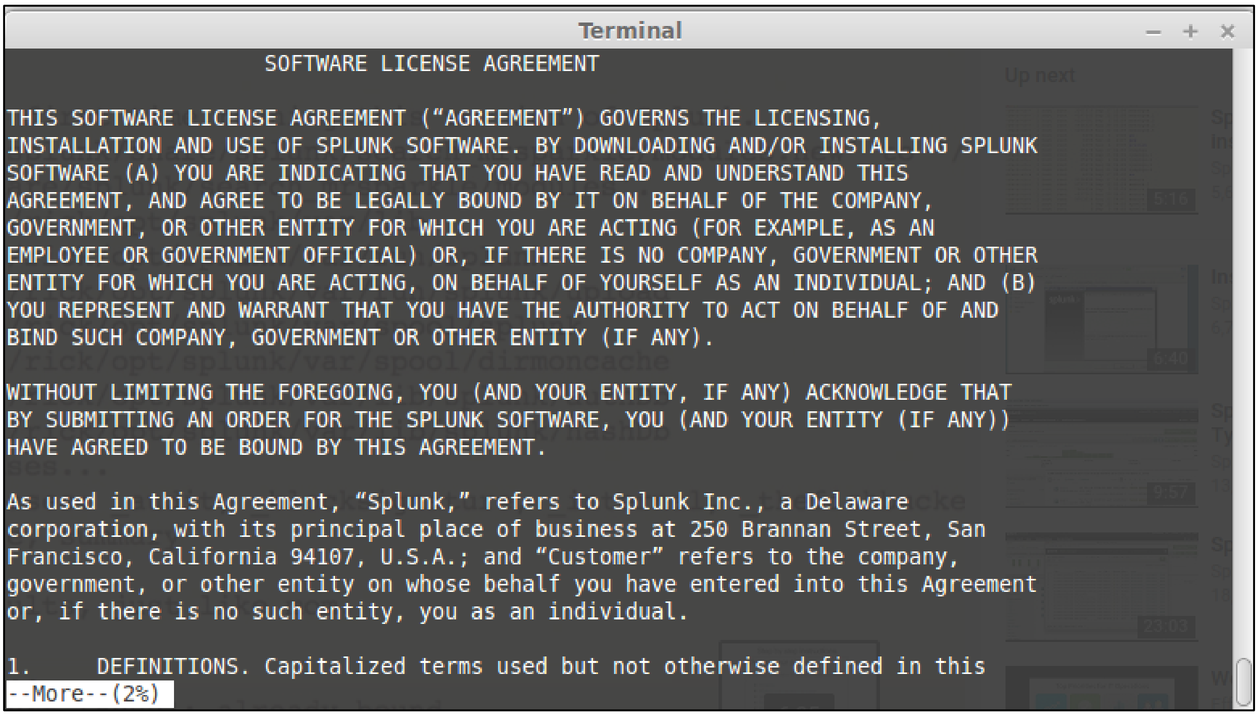


```
splunk/share/splunk/search_mrsparkle/exposed/schema/manager.rnc
splunk/share/splunk/search_mrsparkle/exposed/schema/view.rnc
splunk/share/splunk/search_mrsparkle/exposed/schema/quickstart.rng
splunk/share/splunk/search_mrsparkle/exposed/schema/nav.rng
splunk/share/splunk/search_mrsparkle/exposed/schema/simplexml.rnc
splunk/share/splunk/search_mrsparkle/exposed/schema/advancedxml.xsd
splunk/share/splunk/search_mrsparkle/exposed/schema/all.rnc
splunk/share/splunk/search_mrsparkle/exposed/flash/
splunk/share/splunk/search_mrsparkle/exposed/flash/charting.swf
splunk/share/splunk/search_mrsparkle/exposed/flash/soundmanager2_flash9.swf
splunk/share/splunk/search_mrsparkle/exposed/flash/expressInstall.swf
splunk/share/splunk/search_mrsparkle/exposed/flash/timeline.swf
splunk/share/splunk/search_mrsparkle/exposed/robots.txt
splunk/share/splunk/search_mrsparkle/exposed/xml/
splunk/share/splunk/search_mrsparkle/exposed/xml/print.xml
splunk/share/copyright.txt
guest@Edureka13 ~/Downloads $ cd splunk
guest@Edureka13 ~/Downloads/splunk $ ./splunk start
bash: ./splunk: No such file or directory
guest@Edureka13 ~/Downloads/splunk $ ./start splunk
bash: ./start: No such file or directory
guest@Edureka13 ~/Downloads/splunk $
guest@Edureka13 ~/Downloads/splunk $ cd bin
guest@Edureka13 ~/Downloads/splunk/bin $ ./splunk start
```

These are the other commands that we use commonly:

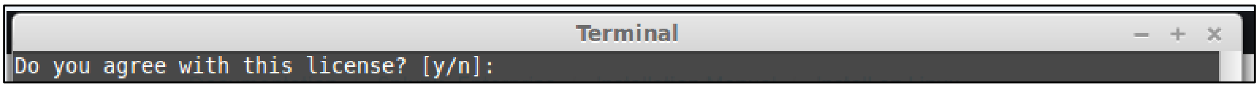
```
./splunk start
./splunk stop
./splunk restart
./splunk help
```

It will ask to agree to the software license agreement as shown:



```
                    SOFTWARE LICENSE AGREEMENT

THIS SOFTWARE LICENSE AGREEMENT (“AGREEMENT”) GOVERNS THE LICENSING,
INSTALLATION AND USE OF SPLUNK SOFTWARE. BY DOWNLOADING AND/OR INSTALLING SPLUNK
SOFTWARE (A) YOU ARE INDICATING THAT YOU HAVE READ AND UNDERSTAND THIS
AGREEMENT, AND AGREE TO BE LEGALLY BOUND BY IT ON BEHALF OF THE COMPANY,
GOVERNMENT, OR OTHER ENTITY FOR WHICH YOU ARE ACTING (FOR EXAMPLE, AS AN
EMPLOYEE OR GOVERNMENT OFFICIAL) OR, IF THERE IS NO COMPANY, GOVERNMENT OR OTHER
ENTITY FOR WHICH YOU ARE ACTING, ON BEHALF OF YOURSELF AS AN INDIVIDUAL; AND (B)
YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO ACT ON BEHALF OF AND
BIND SUCH COMPANY, GOVERNMENT OR OTHER ENTITY (IF ANY).

WITHOUT LIMITING THE FOREGOING, YOU (AND YOUR ENTITY, IF ANY) ACKNOWLEDGE THAT
BY SUBMITTING AN ORDER FOR THE SPLUNK SOFTWARE, YOU (AND YOUR ENTITY (IF ANY))
HAVE AGREED TO BE BOUND BY THIS AGREEMENT.

As used in this Agreement, “Splunk,” refers to Splunk Inc., a Delaware
corporation, with its principal place of business at 250 Brannan Street, San
Francisco, California 94107, U.S.A.; and “Customer” refers to the company,
government, or other entity on whose behalf you have entered into this Agreement
or, if there is no such entity, you as an individual.

1.      DEFINITIONS. Capitalized terms used but not otherwise defined in this
--More--(2%)
```

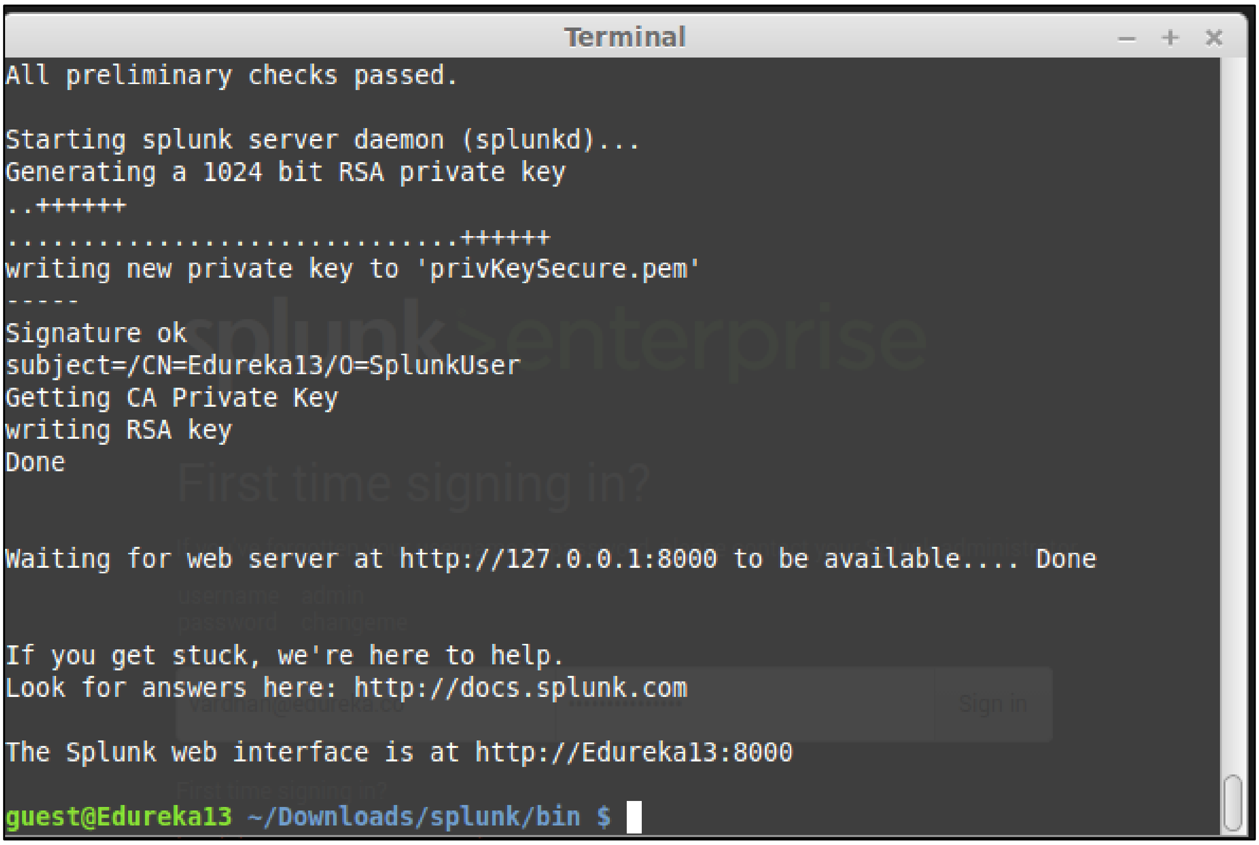
Click on enter.



```
Do you agree with this license? [y/n]:
```

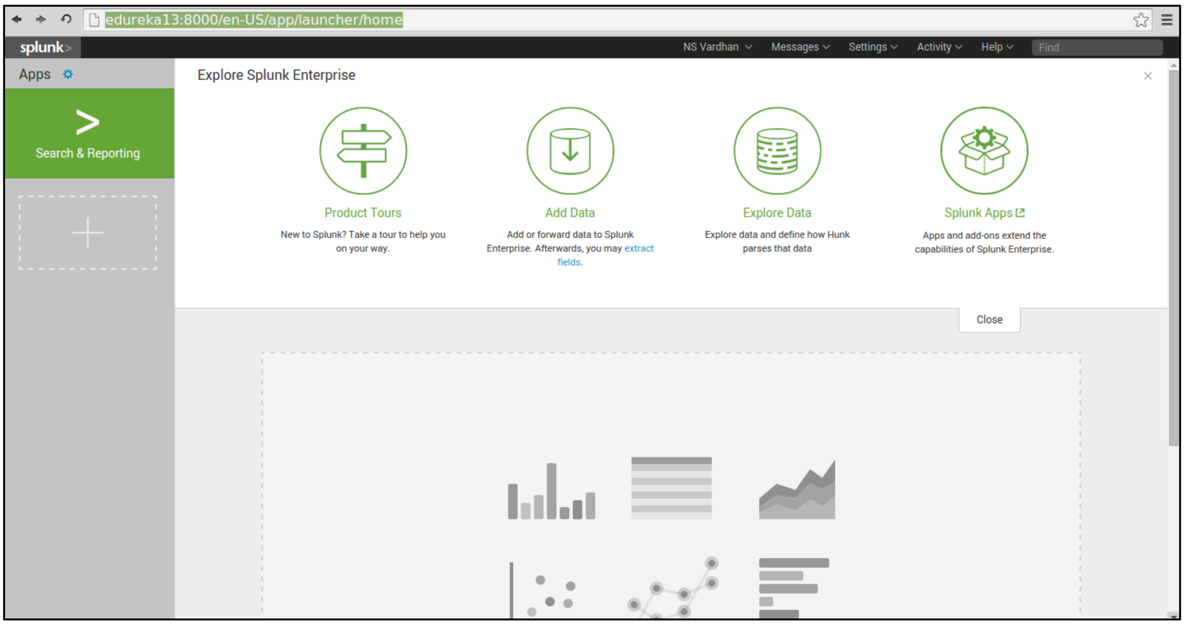
Now click on ‘y’ for agreeing to the terms.

Splunk will be installed successfully as shown below:



```
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a 1024 bit RSA private key
..++++++
..............................++++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=Edureka13/O=SplunkUser
Getting CA Private Key
writing RSA key
Done


Waiting for web server at http://127.0.0.1:8000 to be available.... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://Edureka13:8000

guest@Edureka13 ~/Downloads/splunk/bin $
```

The Splunk web interface is at http://Edureka13:8000. This is the port number, when this is displayed it is indication that connection is established. You will then automatically get connected to the Default Web Browser with that port number as shown below:



Explore Splunk Enterprise

Product Tours

New to Splunk? Take a tour to help you on your way.

Add Data

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Explore Data

Explore data and define how Hunk parses that data

Splunk Apps

Apps and add-ons extend the capabilities of Splunk Enterprise.