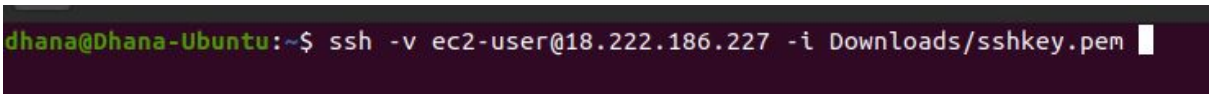
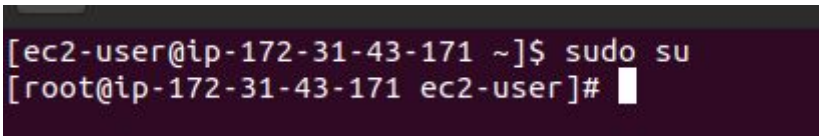
Splunk Installation

- To Create Instances/Servers I have used Amazon Web Services(AWS)
- I have created AWS account
- After creating aws account I Have Lanched 4 EC2 Instances
- All Instances are RedHat 8 Platform
- While Setting up those instances *.pem file has been Downloaded
- After successful download changing the *.pem file permissions to give
  Chmod 400 sshkey.pem because security reasons
  Otherwise you can't connect EC2 Instances
- I get Inside the server i have used Command Line Interface
- CLI I have mentioned IP address of the Instance that I have already created in AWS
- CLI Enter The Following These Steps
- 

- I have logged into server terminal as ec2-user

- Then I have Changed ec2-user to root-user

- 
```
[ec2-user@ip-172-31-43-171 ~]$ sudo su
[root@ip-172-31-43-171 ec2-user]#
```

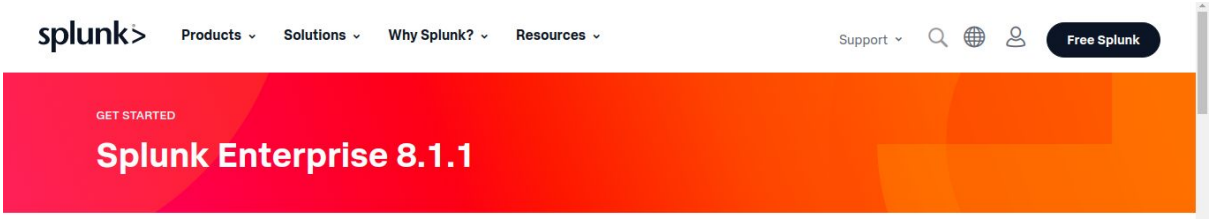
- Update System repository Index First:

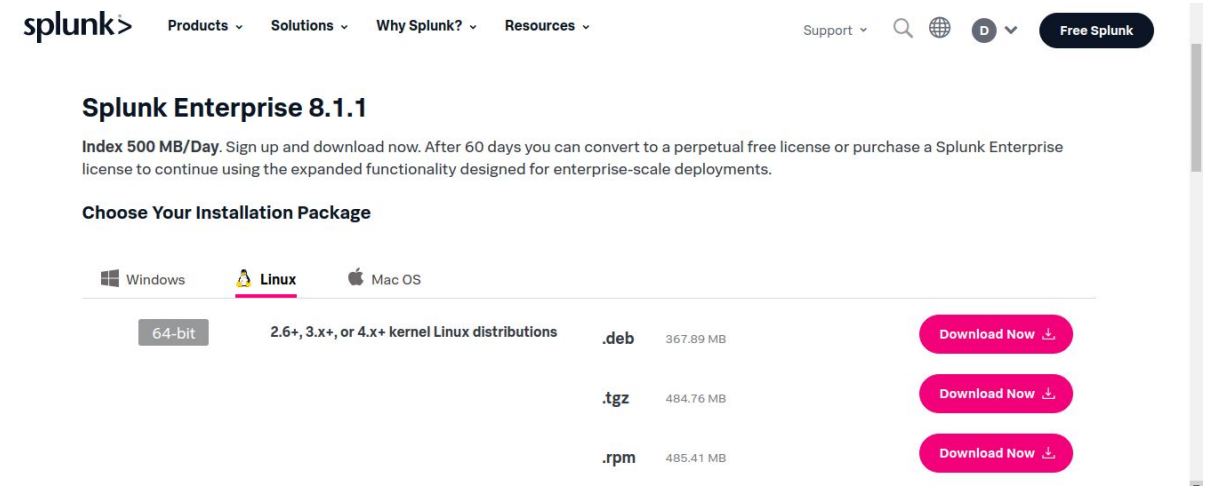
```
[root@ip-172-31-43-171 ec2-user]# sudo yum update
Last metadata expiration check: 1:09:18 ago on Monday 11 January 2021 06:00:22 AM UTC.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-172-31-43-171 ec2-user]#
```

- Next to install Splunk I have downloaded the wget by using the below command:

```
[ec2-user@ip-172-31-43-171 ~]$ sudo yum install wget -y
Last metadata expiration check: 1:15:50 ago on Monday 11 January 2021 06:00:22 AM UTC.
Package wget-1.19.5-10.el8.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-43-171 ~]$ cd /opt
[ec2-user@ip-172-31-43-171 opt]$
```

- Then to install Splunk enterprise Version I have created an account I Splunk website.





- In Tools page Splunk website I have copied the below command pasted in the server

-
```
[root@ip-172-31-43-171 opt]# wget -O splunk-8.1.1-08187535c166-Linux-x86_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_
[root@ip-172-31-43-171 opt]# wget -O splunk-8.1.1-08187535c166-Linux-x86_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=8.1.1&product=splunk&filename=splunk-8.1.1-08187535c166-Linux-x86_64.tgz&wget=true'
```

- Then the Splunk software was downloaded. To get that installed I have used the below command

-
```
[root@ip-172-31-43-171 opt]# tar -xvzf splunk-8.1.1-08187535c166-Linux-x86_64.tgz
```

- Then to start Splunk I used the below command and added the password.

-
```
[root@ip-172-31-43-171 opt]# cd splunk/bin
[root@ip-172-31-43-171 bin]# ./splunk start --accept-license
```
At the time asking username and password

- I have used the following commands to stop and start Splunk.

```
[root@ip-172-31-43-171 bin]# ./splunk stop
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
...                                                        [  OK  ]
Stopping splunk helpers...
                                                           [  OK  ]
Done.
[root@ip-172-31-43-171 bin]#
```

- Start Splunk

```
[root@ip-172-31-43-171 bin]# ./splunk start

Splunk> Like an F-18, bro.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8090]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-8.1.1-08187535c166-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                           [  OK  ]

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://ip-172-31-43-171.us-east-2.compute.internal:8000
```