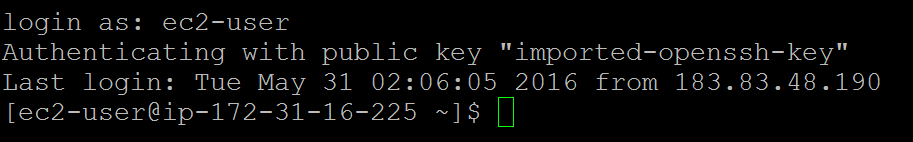
**Splunk Universal Forwarder Installation**

1. Login to the server as “**ec2-user**”



1. Jump to root user using “**sudo su**” and do the prerequisites for SplunkForwarder Installation

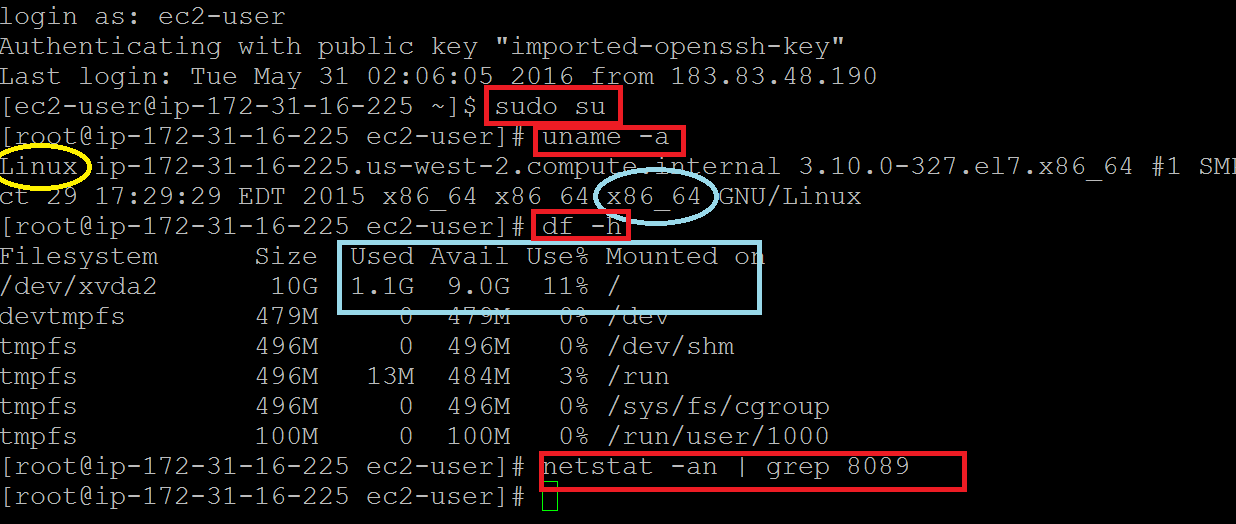
Splunk can run as any user on the local system. If you run Splunk as a non-root user, make sure that Splunk has the appropriate permissions to read the inputs that you specify.

Check the OS and architecture using “**uname –a**”. It is necessary to download the appropriate package

Check the space availability in opt. Splunk requires 1GB of free space atleast. First preferable mountpoint would be /opt. If it is not free then go with other mountpoint which is having 1GB of free space

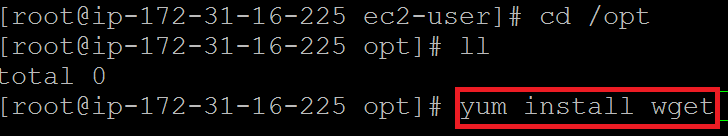
To check the free space use “**df –h**”

Check whether Splunk Default Management port is already in use or not using netstat command. If it is used by any other process then change it to available ports



1. Go to opt folder and list it. Nothing will be here as of now. Now we are going to download our Splunk Forwarder package here using “**wget**”

wget is an utility which retrieves content from web servers. It is not present by default in some systems. So download it using “**yum install wget**”

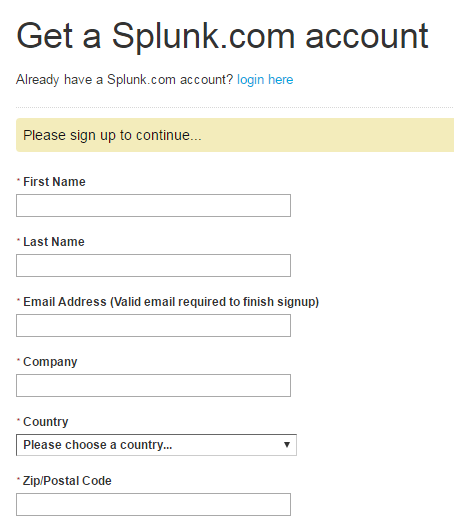
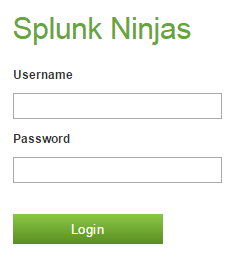


1. Go to the below URL to download the UF package and click on appropriate OS and architecture

For Forwarder Installation <https://www.splunk.com/en_us/download/universal-forwarder.html>

For Full Installation <https://www.splunk.com/en_us/download/splunk-enterprise.html>

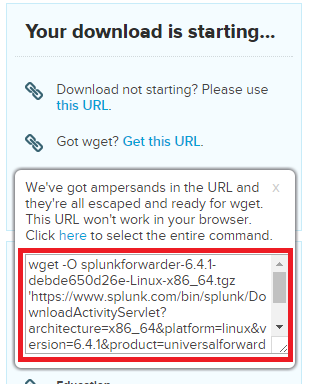
You need Splunk account to download it. Sign up for new account or login with credentials if you already have

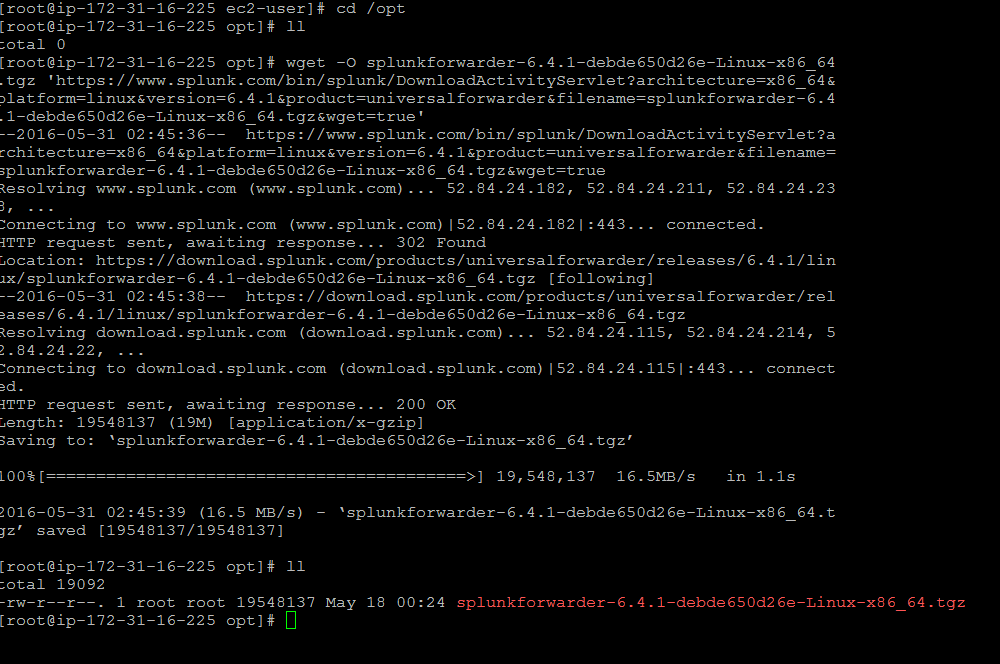
 

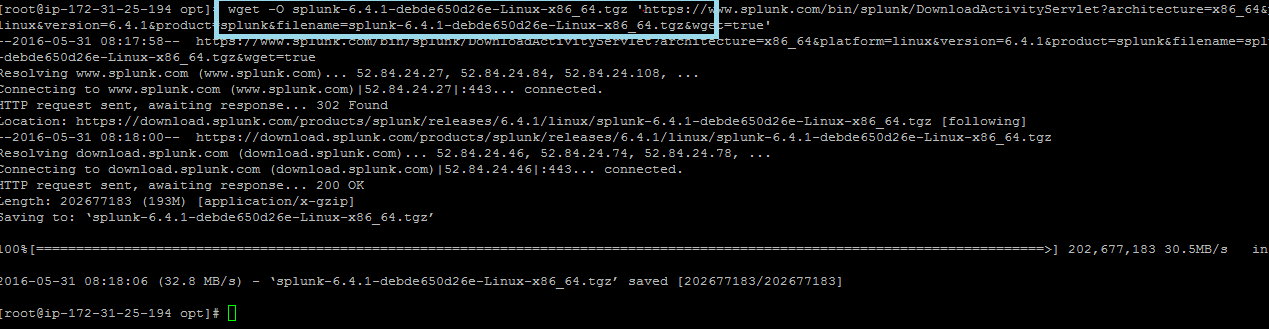
1. Package is getting downloaded. You could move manually from your local desktop to Target Box using WinSCP tool

The best and easy way is to download via wget utility. Once it started to download you will find a wget url in the right hand side.

Copy the contents and paste it in your server and press Enter



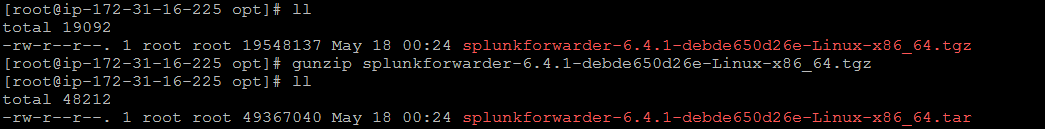


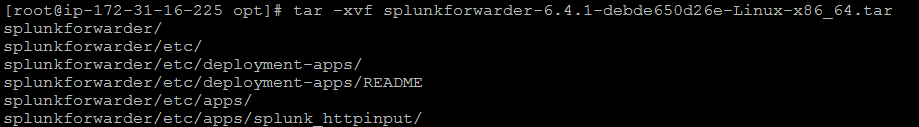


1. Now the tar package has been downloaded in your server. It needs to be unzipped and untar using the below commands

**“gunzip <package name>”**

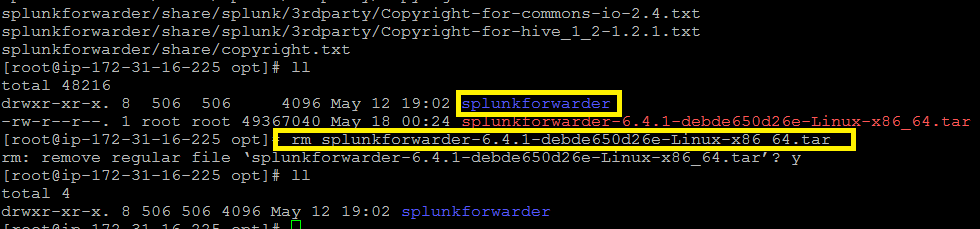
**“tar –xvf <tar package name>”**

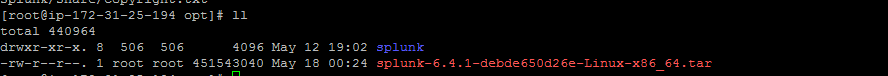




1. Now “splunkforwarder” folder has been extracted out of package. Remove the tar file carefully using the “**rm**” command”

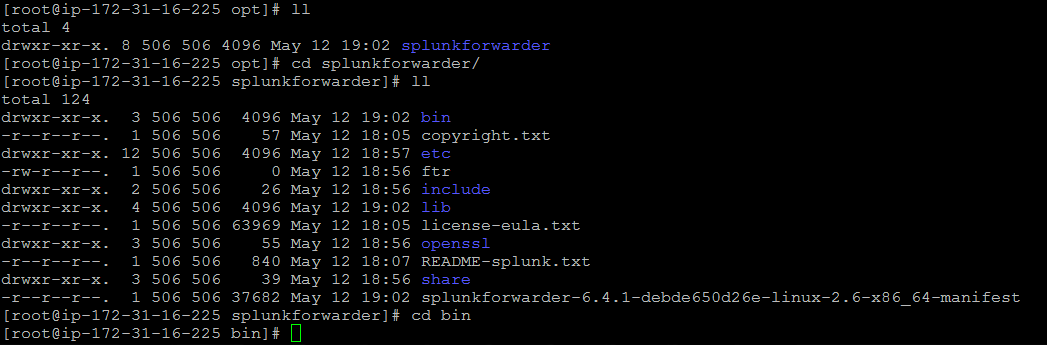
Package has been installed successfully





**Start the splunkforwarder service**

1. Go to the splunkforwarder folder then bin directory



1. From bin directory you are able to do the CLI commands

**./splunk start ----- To start**

**./splunk stop ------- To stop**

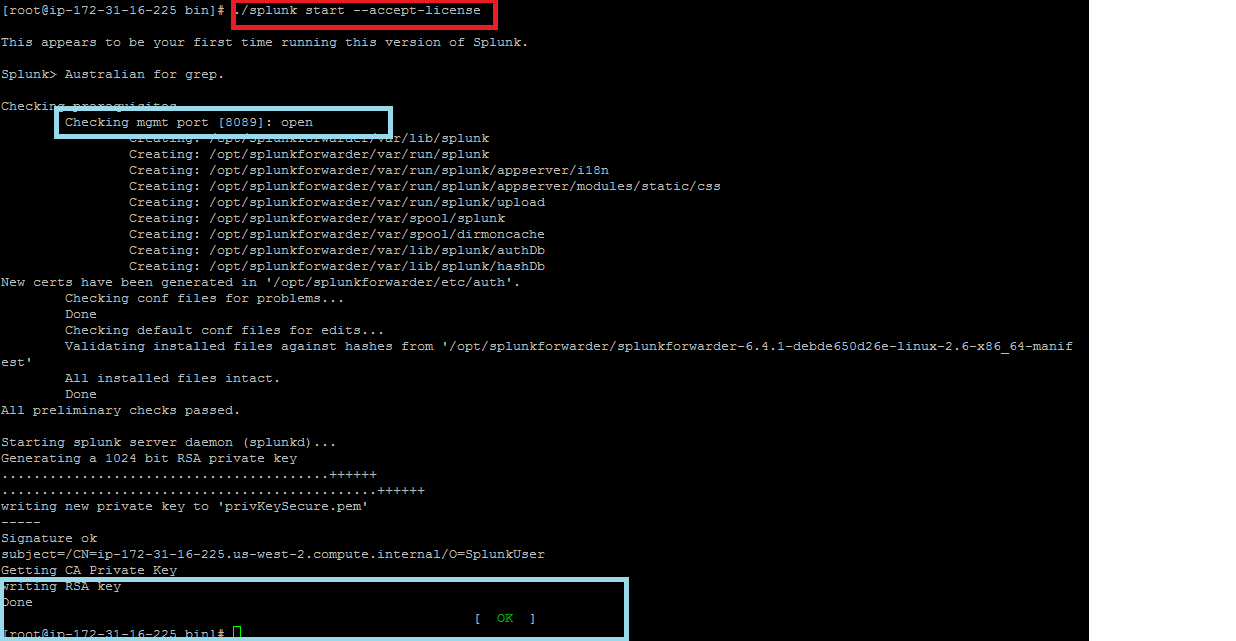
**./splunk restart ----- To restart**

**./splunk status ------- To check status**

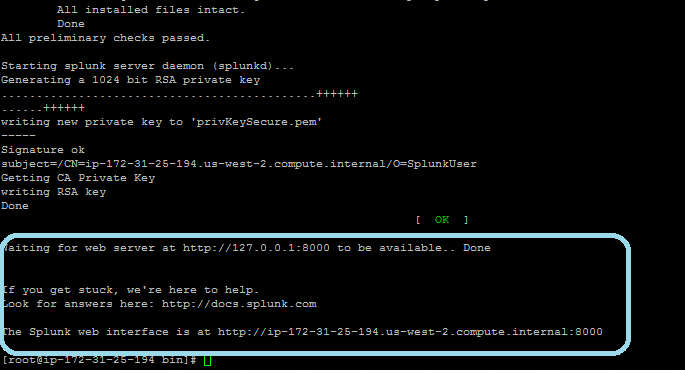
**./splunk version ----- To check version**

Note : For first time start give the command as below to bypass the license agreement

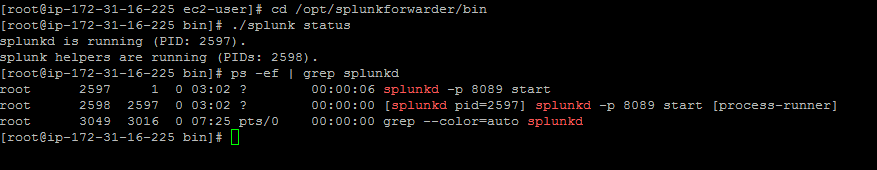
**“./splunk start –accept-license”**







Now move to the bin folder and check the status



Now again test the port is listening on 8089

