**Installing Splunk**

Splunk is one the best SIEM solutions out there. A SIEM is a very component for any enterprise security. It allows managing all machine data or logs in a centralized location. The best thing about Splunk they let you have the full Splunk enterprise experience for 90 days for free. In this I am going to do two things

1. Create a virtual machine (Ubuntu server)
2. Install Splunk enterprise in the VM

**Requirements**

* Virtual box installed
* Knowledge on how to create a VMs in virtual box
* Internet access

1-Create a virtual Ubuntu machine and download the Ubuntu Server ISO file.

**VM specifications:** 2048 MB of RAM, minimum of 80GB if hard drive and make sure the network adapter is on bridged adapter. Download the Ubuntu server ISO [here](https://ubuntu.com/download/server). Make sure you pick the latest version.

After you finished downloading the ISO file, you need to attach it the hard drive of the VM, power up the VM and follow the instruction to install Ubuntu server. Make sure you select install SSH during the installation process.

When the installation process is completed, login into your server using the username and password set during the installation. Before you do anything else you need make sure you update the server by running these commands:

* **Sudo apt update**
* **Sudo apt upgrade**

Just in case you missed the SSH step during the installation, you can install SSH and net-tools with this command:

* **Sudo apt install SSH**
* **Sudo apt install net-tools**

**Find out you server IP address with this command:**

* **ipconfig**

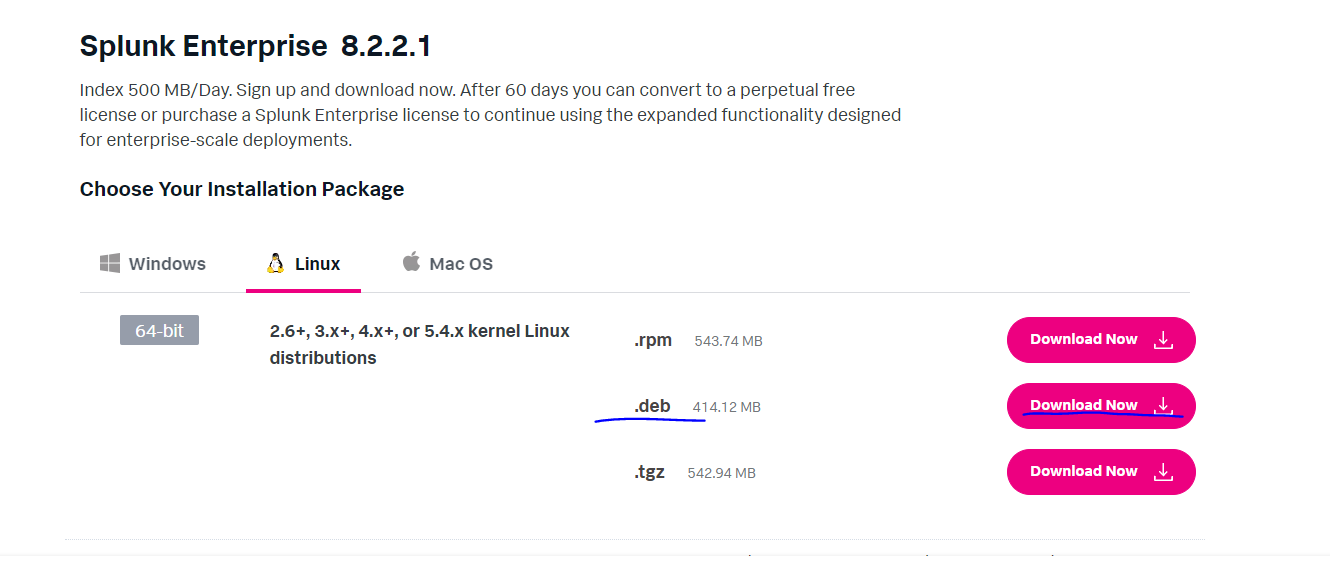
The server is ready now. It is time to install Splunk. To do that, we are going to SSH into the server using PowerShell in our host machine. We are doing that because we want to use copy and paste feature.

2-Installing Splunk

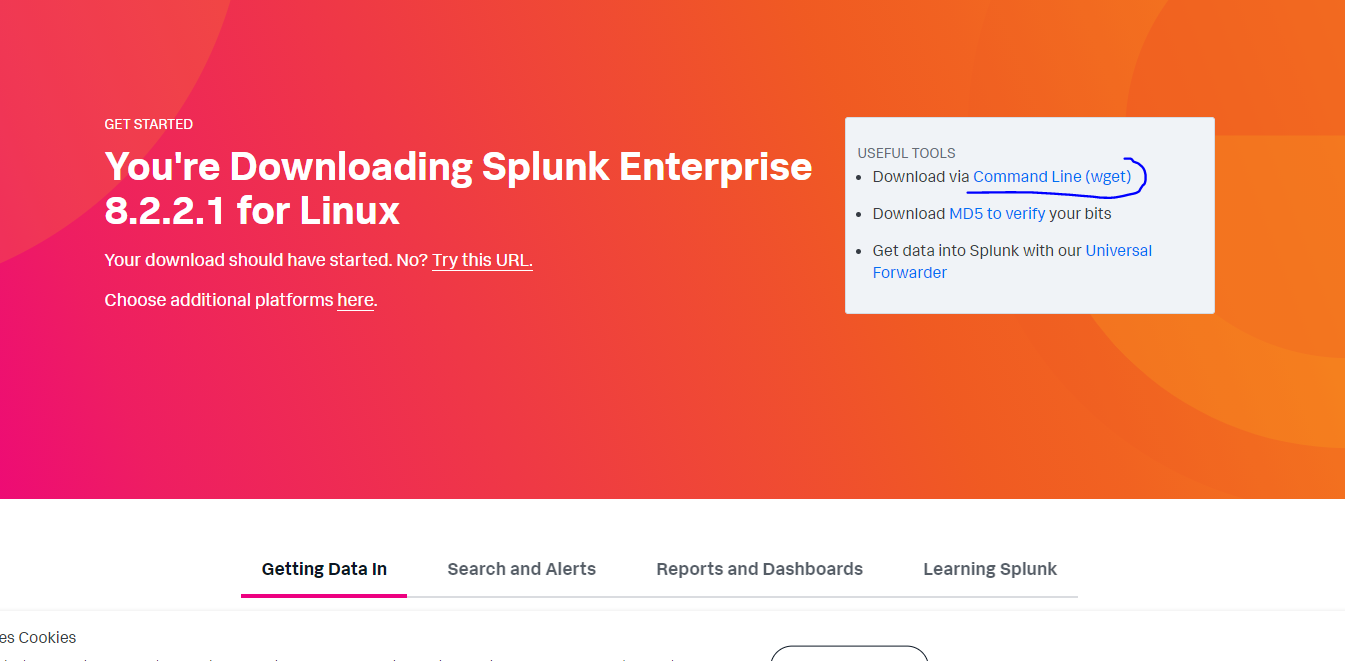
First you need go the [splunk website](https://www.splunk.com/)  and signup to open an account



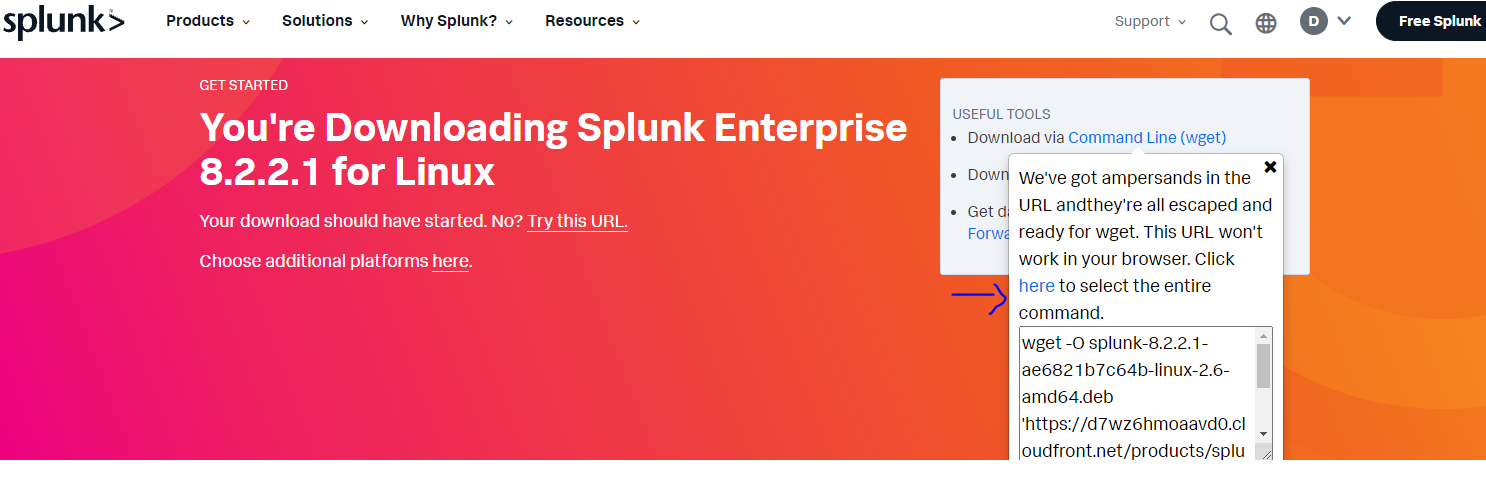
After login click on free trial and choose your operating system. In our case we choose Linux and download the .deb extension



Once you click download, the download dialogue will popup. At this stage we can cancel it if you want because we going to use the command line instead to install Splunk. Click on download via command like wget.



Click here to copy the code and paste it into the SSH session to your sever to download splunk.



3-At this stage Splunk should be downloaded in your home directory. You can use this command to install it in the current directory.

* **Sudo dpkg –I splunk-8.2.2.1-ae6821b7c64b-linux-2.6-amd64.deb**

Splunk should be installed in /opt/splunk

4- Let start splunk using this command:

* **Sudo /opt/splunk/bin/splunk start–accept-license**
* **sudo /opt/splunk/bin/splunk enable boot-start**

During the installation process you will be asked to provide administration password. And username

5- Next step will be setting up SPLUNK\_HOME as a system-wide variable. You need to edit etc/environment. You can use the editor of your choice to that. Just make to include the following line:

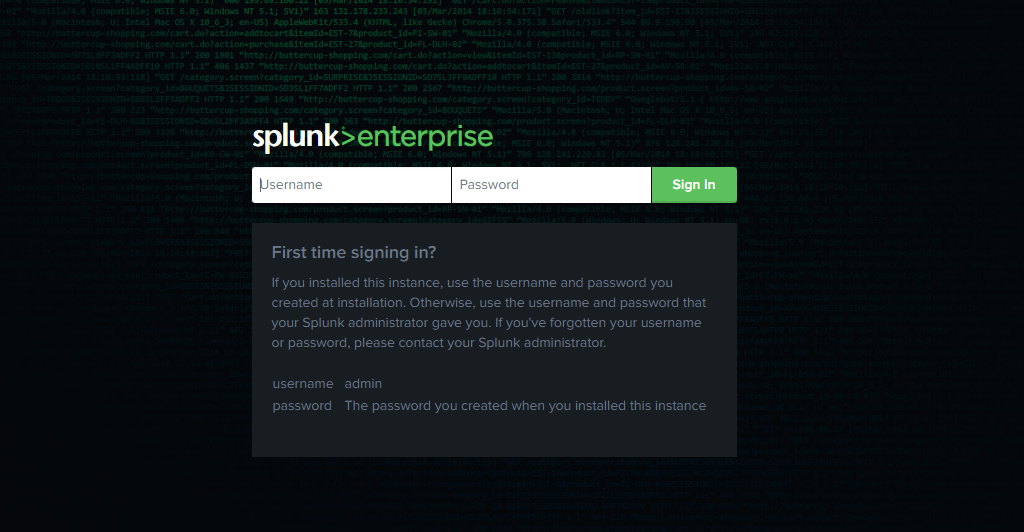
**SPLUNK\_HOME=“/opt/splunk”**

Now you can save the file and close it.

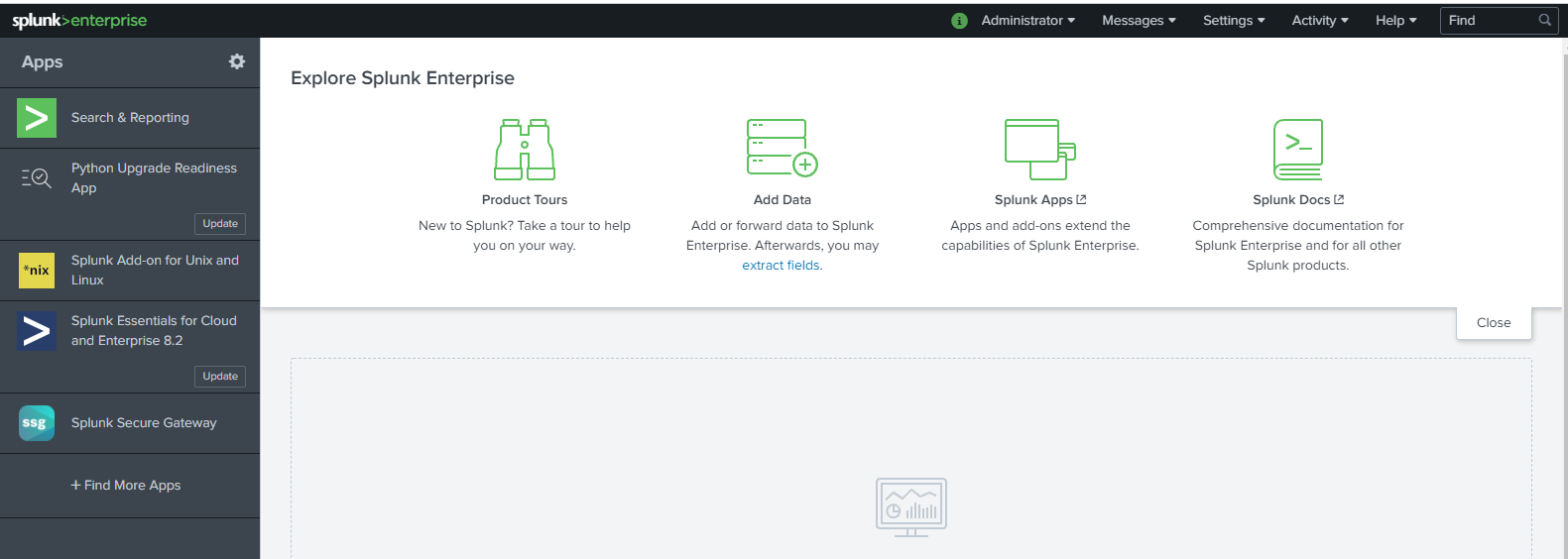
6-Splunk is now installed and running. It is time now to access and the splunk experience. Open a new tab in the bowser in your host machine and type:

* <http://”your> splunk server IP address”:8000

Mine is as follow <http://192.168.1.14:8000>



Use the admin username and password to login.



Voila! Now we are login into Splunk enterprise.