Installing Splunk

Splunk is one of the best SIEM solutions out there. A SIEM is a very important component for any enterprise security. It allows managing all machine data or logs in a centralized location. The best thing about Splunk is they let you have the full Splunk enterprise experience for 90 days for free. In this lab, 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 of hard drive and make sure the network adapter is on the bridged adapter. Download the Ubuntu server ISO here. Make sure you pick the latest version.

After you finished downloading the ISO file, you need to attach it to the hard drive of the VM, power up the VM, and follow the instructions to install the 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 to 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**

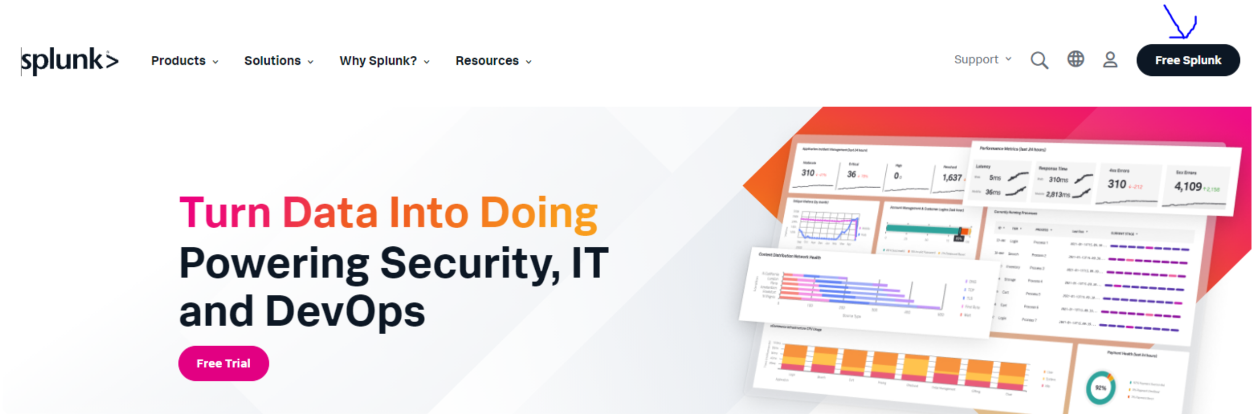
You can find out your server IP address with this command:

- **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 a copy and paste feature.

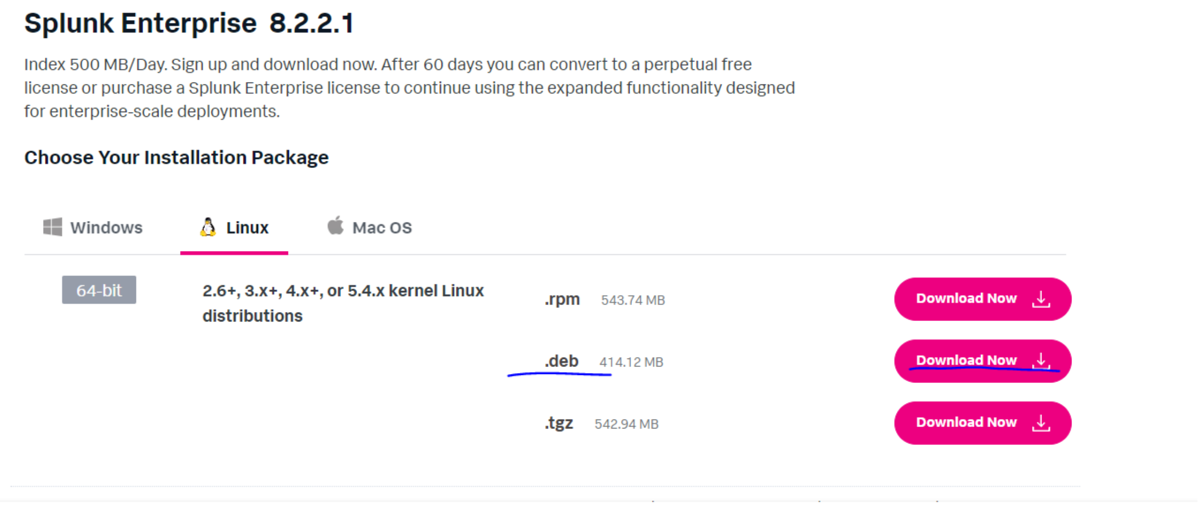
2-Installing Splunk

First, you need to go to the Splunk website and signup to open an account



Turn Data Into Doing
Powering Security, IT and DevOps

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



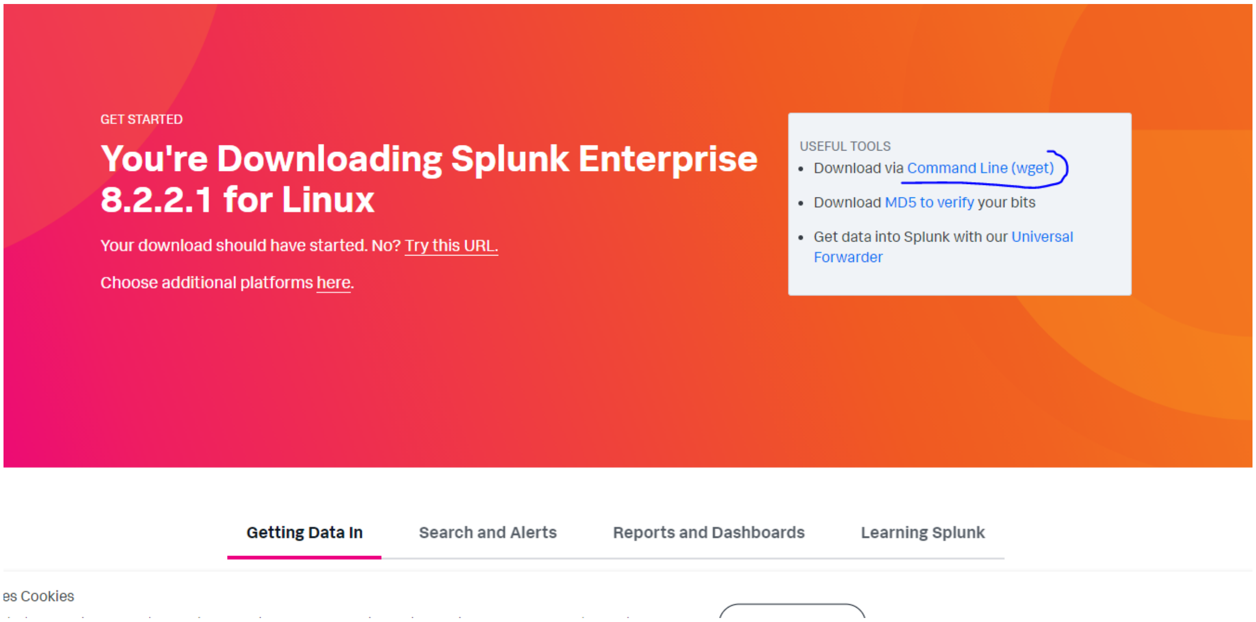
Splunk Enterprise 8.2.2.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

64-bit	2.6+, 3.x+, 4.x+, or 5.4.x kernel Linux distributions	.rpm	543.74 MB	Download Now
		.deb	414.12 MB	Download Now
		.tgz	542.94 MB	Download Now

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



GET STARTED

You're Downloading Splunk Enterprise 8.2.2.1 for Linux

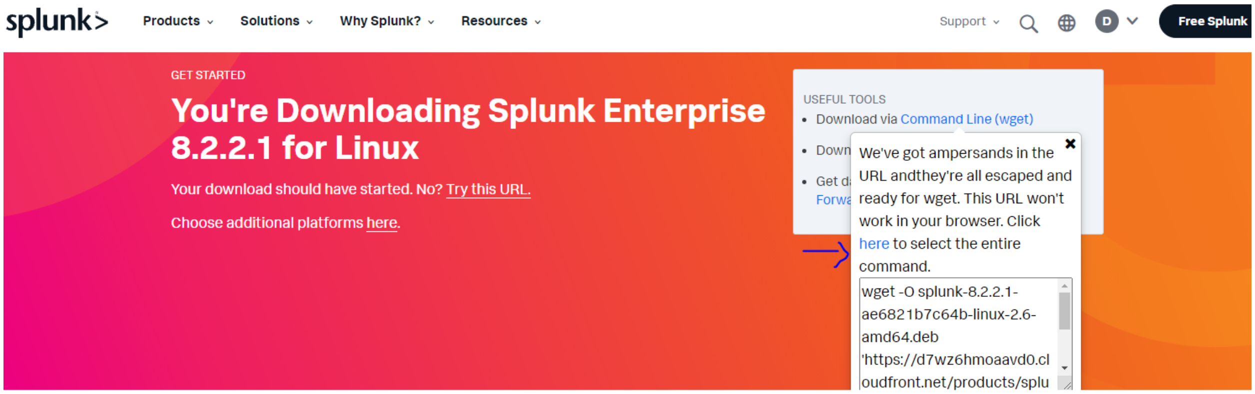
Your download should have started. No? Try this URL.

Choose additional platforms here.

USEFUL TOOLS

- Download via Command Line (wget)
- Download MD5 to verify your bits
- Get data into Splunk with our Universal Forwarder

Click **here** to copy the code and paste it into the SSH session to your server to download Splunk.



GET STARTED

You're Downloading Splunk Enterprise 8.2.2.1 for Linux

Your download should have started. No? Try this URL.

Choose additional platforms here.

USEFUL TOOLS

- Download via Command Line (wget)
- Down
- Get d Forwa

We've got ampersands in the URL andthey're all escaped and ready for wget. This URL won't work in your browser. Click here to select the entire command.

```
wget -O splunk-8.2.2.1-
ae6821b7c64b-linux-2.6-
amd64.deb
'https://d7wz6hmoaavd0.cl
oudfront.net/products/splu
```

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 an administrator 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 do that. Just make to include the following line:

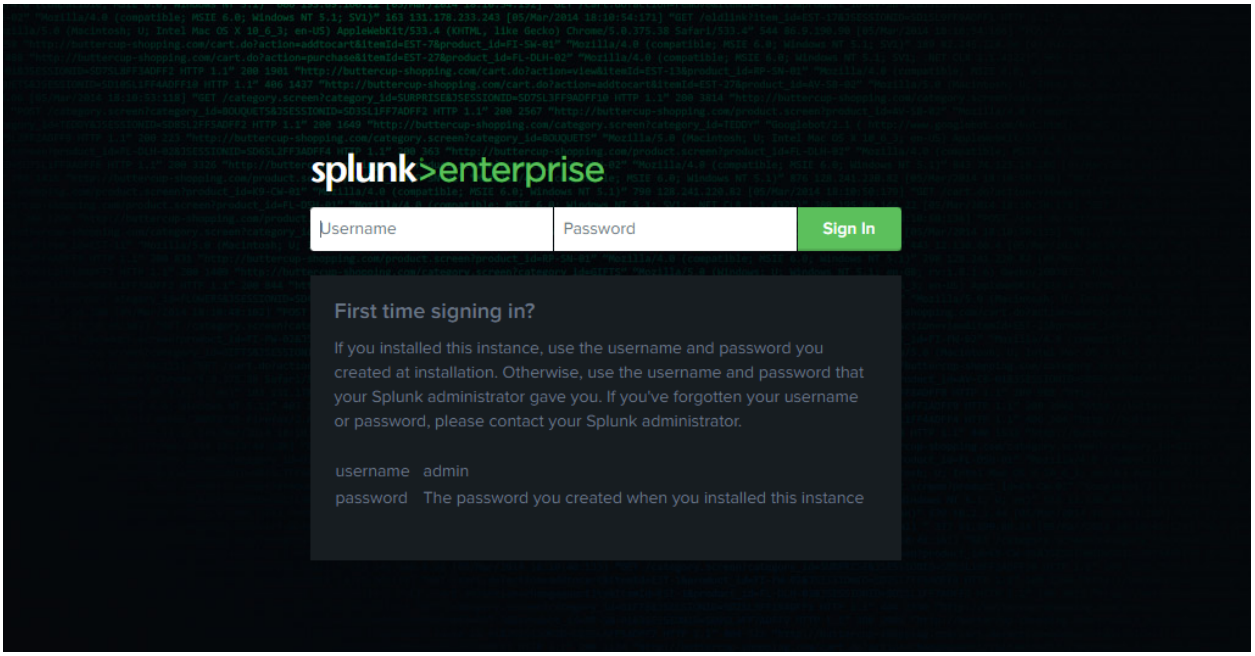
SPLUNK_HOME="/opt/splunk"

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 browser in your host machine and type:

- **http://"your splunk server IP address":8000**

Mine is as follow http://192.168.1.14:8000

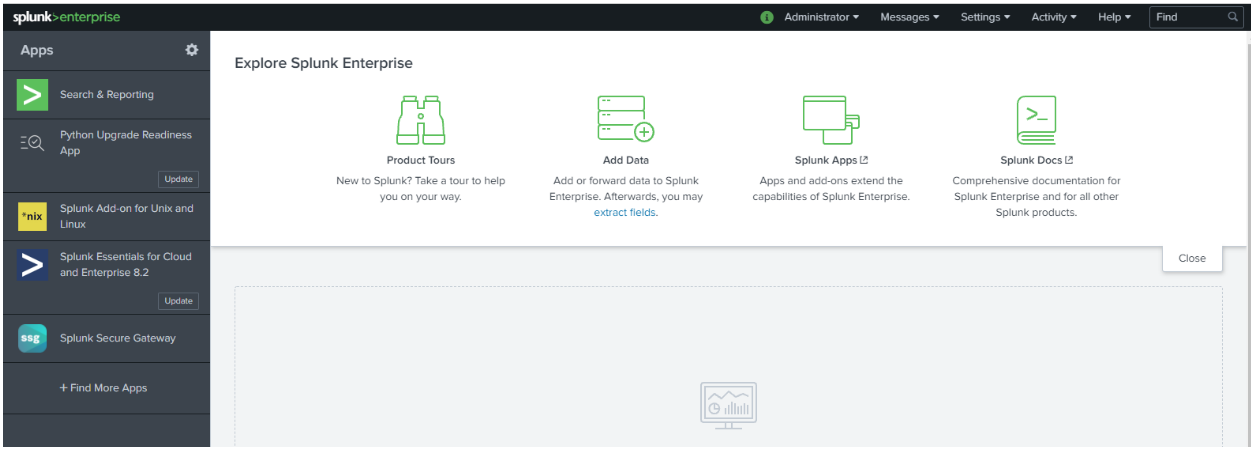


First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

Use the admin username and password to log in



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.

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

Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

Voila! Now we are login into Splunk enterprise.