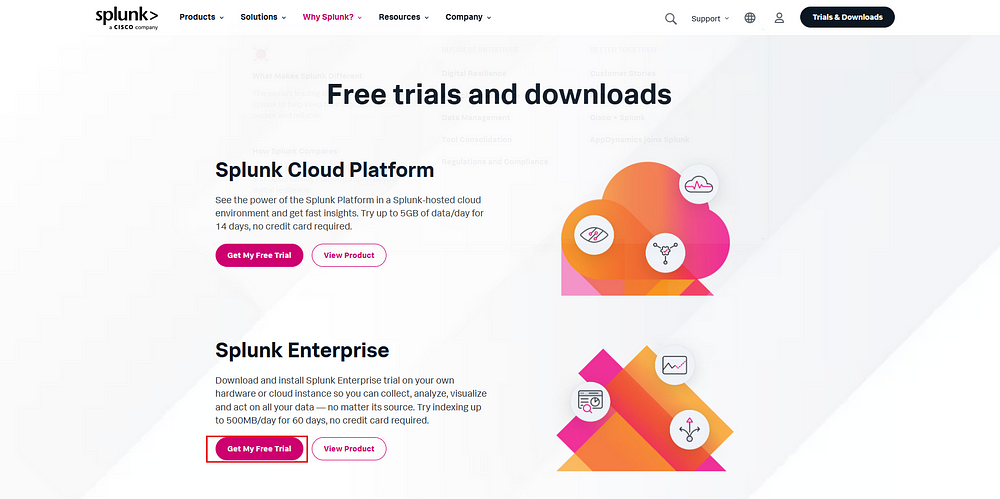
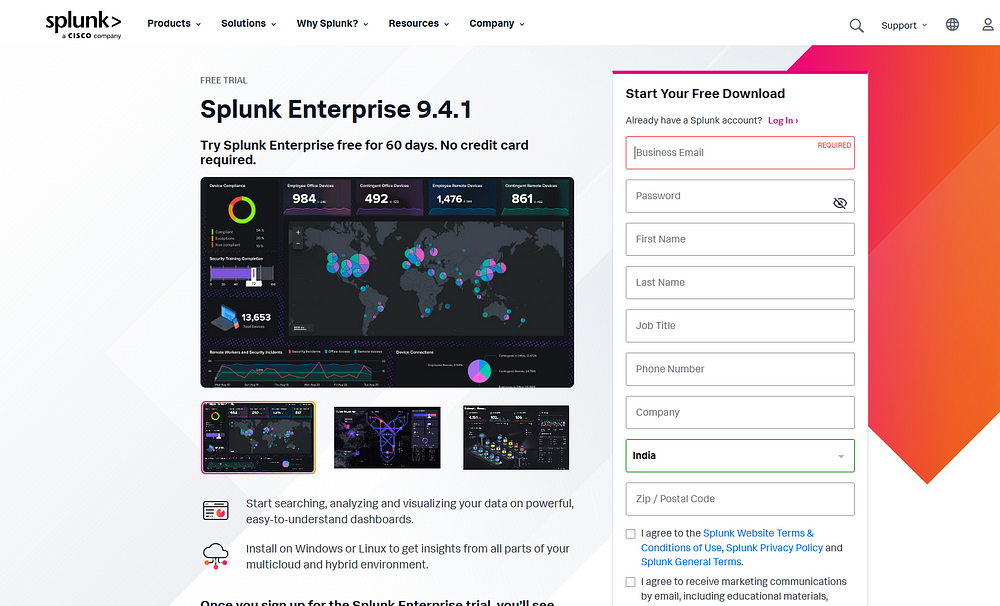
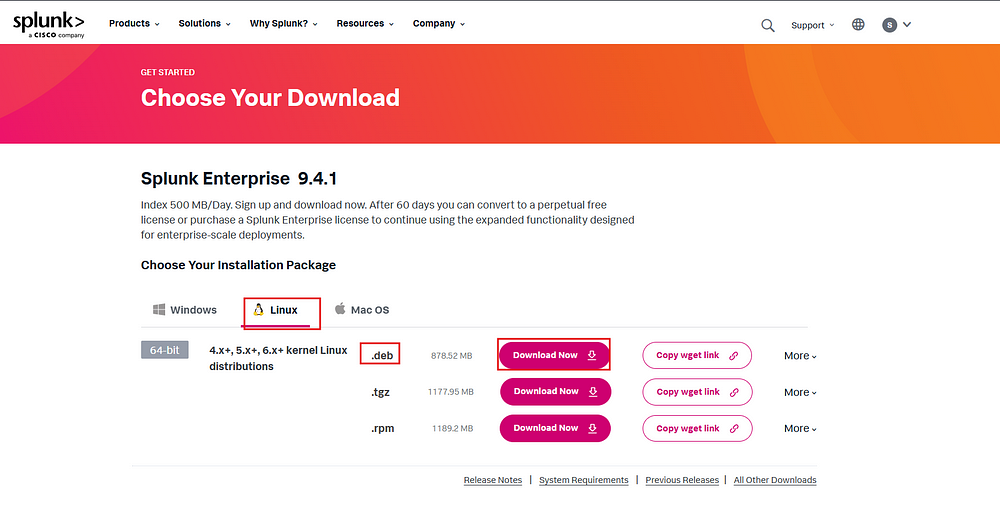
### **Splunk Installation**

Download the Splunk enterprise from [here](https://www.splunk.com/en_us/download.html). Click on the “Get My Free Trial” option.

Enter the details and create an account.

Verify the account and download the splunk enterprise for Linux.

Now, on the ubuntu server, enter the following command

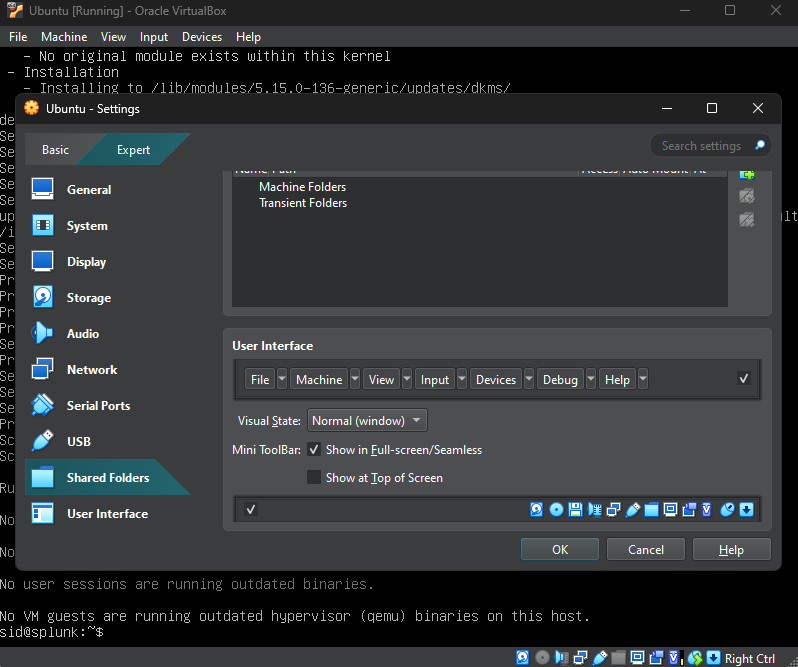
sudo apt-get install virtualbox-guest-additions-iso

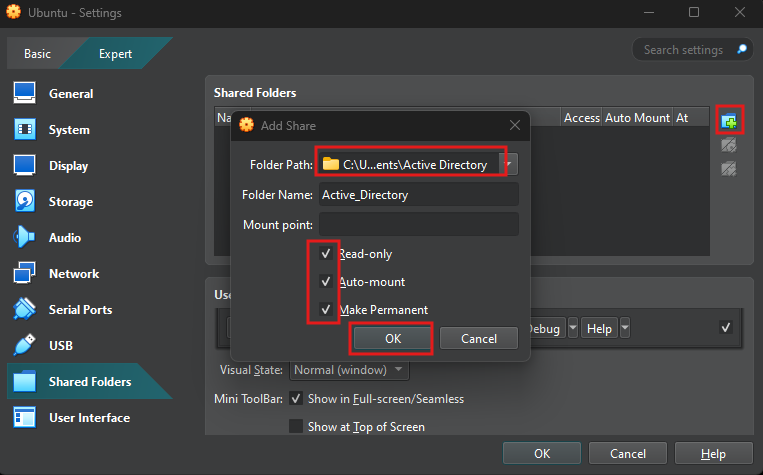
Enter you password. When prompted press Y.

Then enter the following command

sudo apt-get install virtualbox-guest-utils

Once the installation is complete, in the virtual box menu bar go to Devices -> Shared Folders -> Shared Folder Settings.

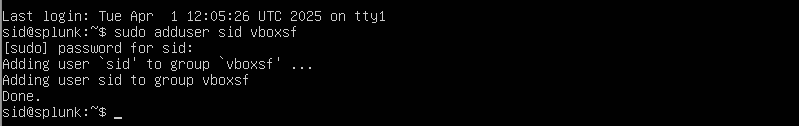
Before this place the Splunk download in a separate folder. Once in the settings select new and then select the path to the folder where Splunk is downloaded. Then check all three check boxes and click ok.

Now, reboot the VM using the following

sudo reboot

Once rebooted, log back in and type the following command to add the user to vboxsf.

sudo adduser <username> vboxsf



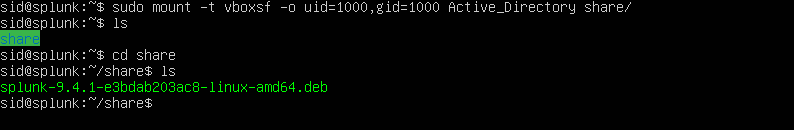
Then create a folder named share

mkdir share

Now we have to mount our shared folder to the share folder. We can do this by entering the following command

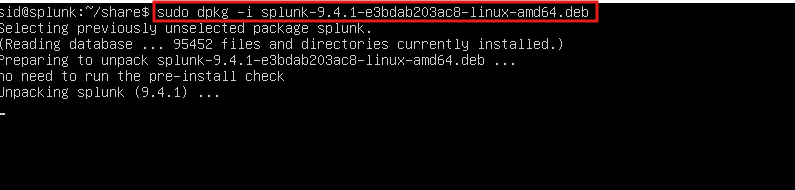
sudo mount -t vboxsf -o uid=1000,gid=1000 <shared\_folder\_name> share/

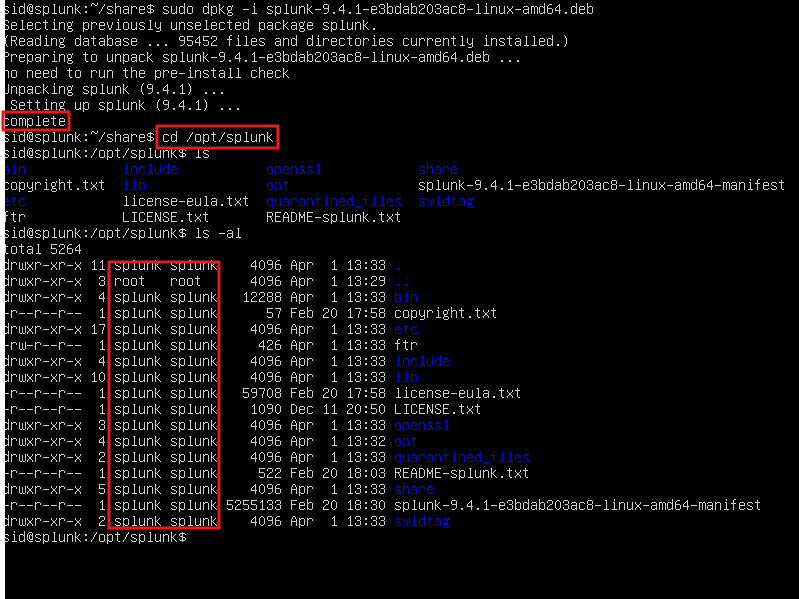
Now if we cd into the share folder and then list the files with ls we can see our Splunk download.



Now, we can install splunk by using the below command

sudo dpkg -i splunk-9.4.1-e3bdab203ac8-linux-amd64.deb

Once the download is complete we can navigate into the Splunk folder under /opt/splunk.

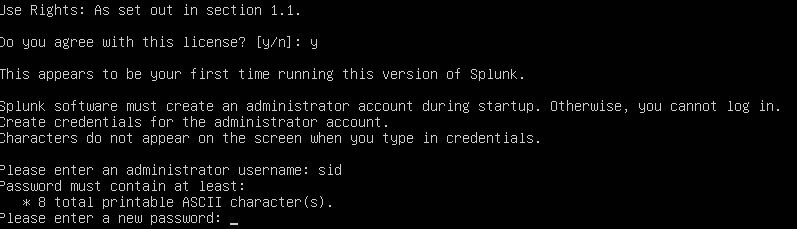
As we can see above all the splunk file are under user splunk. Now we can change the user to splunk using the following command

sudo -u splunk bash

Once the user is changed, navigate to bin folder and type the following to run the Splunk installer

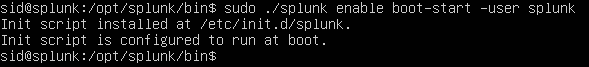
./splunk start

when prompted, accept the license agreement by typing y. Then enter the admin username and password you want to use.

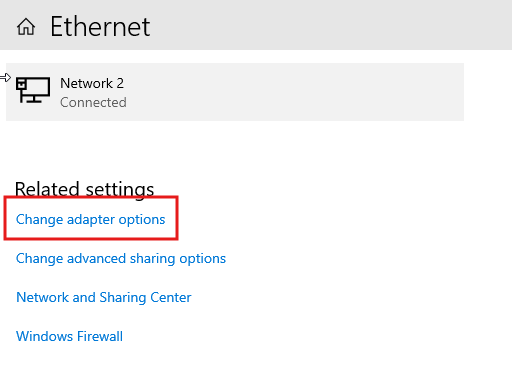


Now we should enable Splunk to start on boot. We can do this by exiting Splunk and then typing the following command.

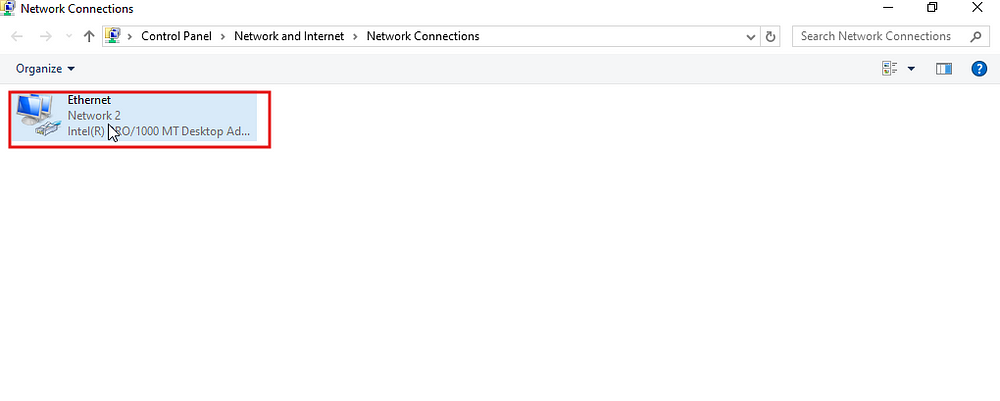
sudo ./splunk enable boot-start -user splunk

Splunk on **7.Sysmon and Splunk Forwarder install on Windows machine**

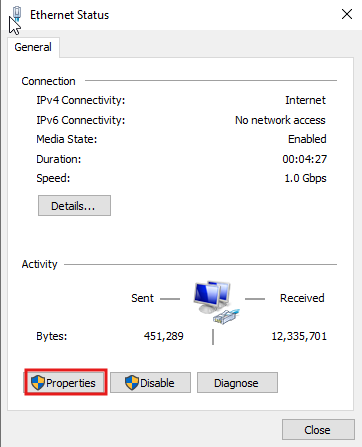
First let us set the IP address of the machine to reflect the network diagram. Go to ethernet settings and click on Change adapter options



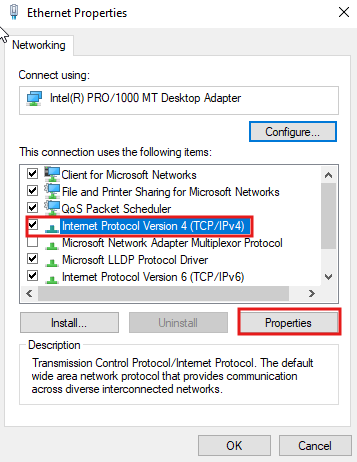
Then double click on the adapter.



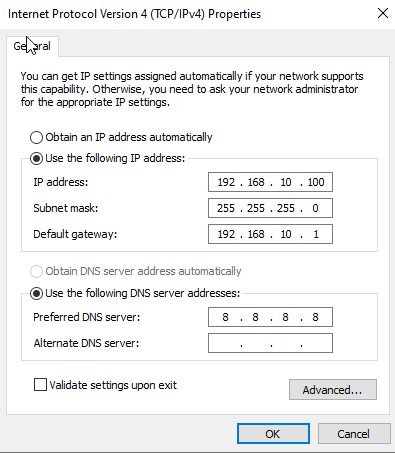
Then select properties.



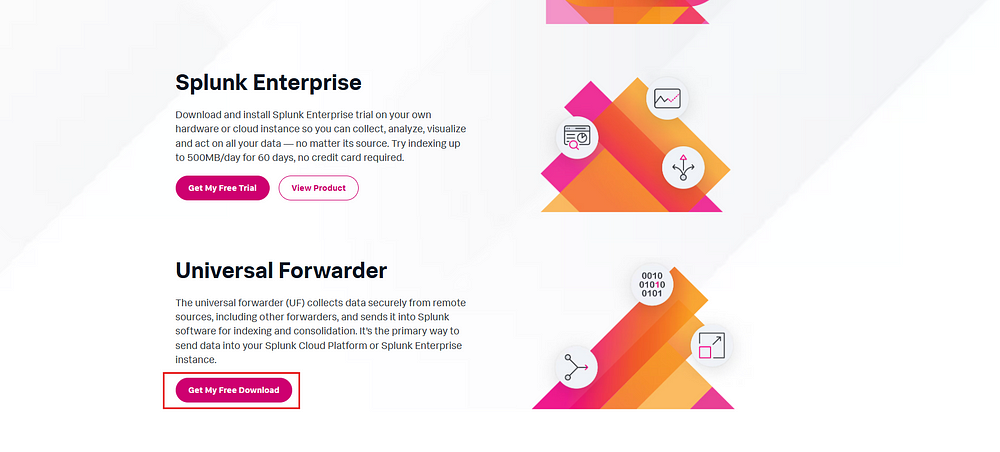
Then select IPv4 and properties.



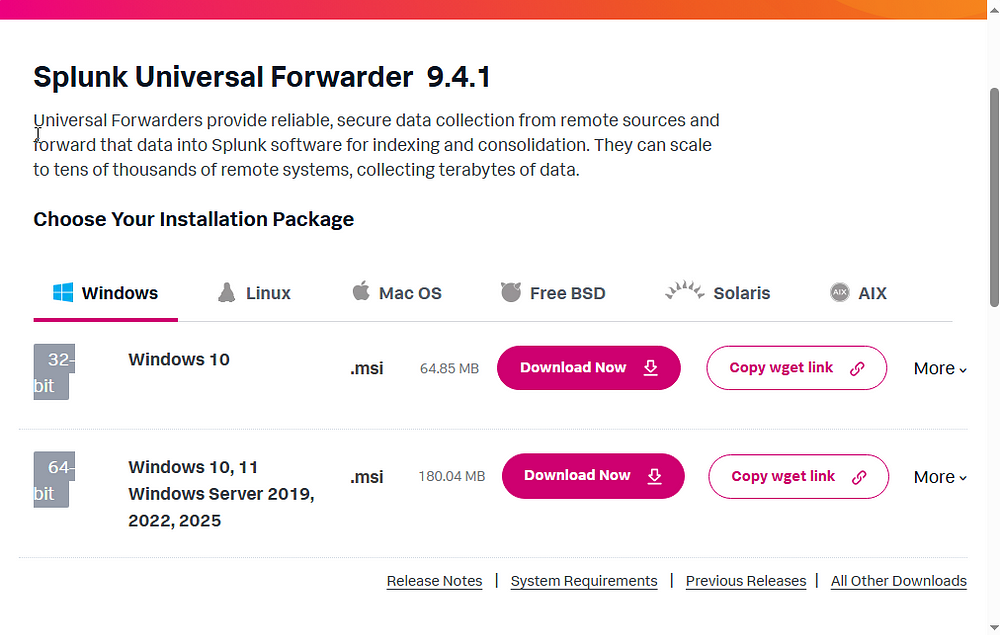
Then enter the following configuration and click ok.



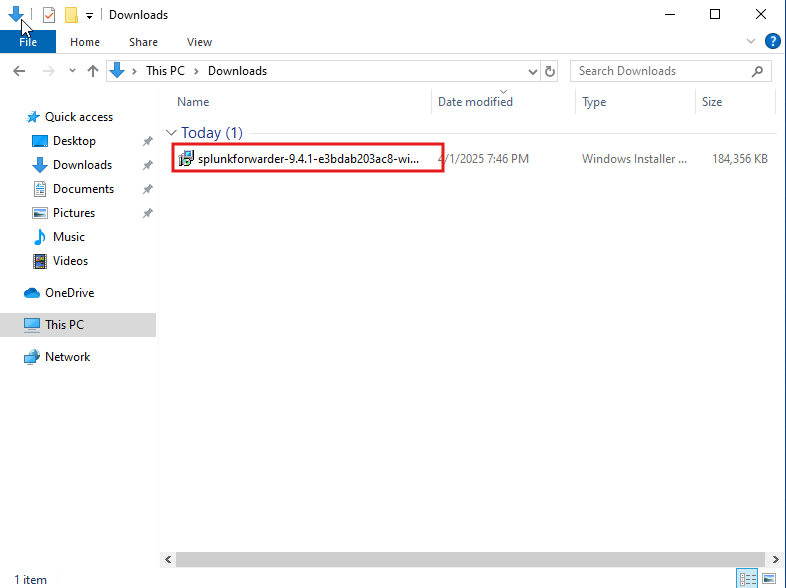
Once done, we can download the Splunk universal forwarder in this machine by visiting this [site](https://www.splunk.com/en_us/download.html) and signing in.

Splunk Universal forwarder download

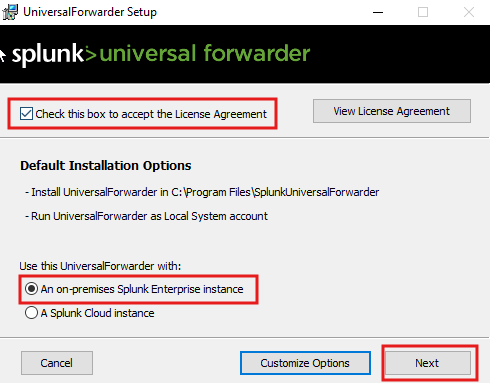
Select the appropriate version to download.

Splunk Universal forwarder download

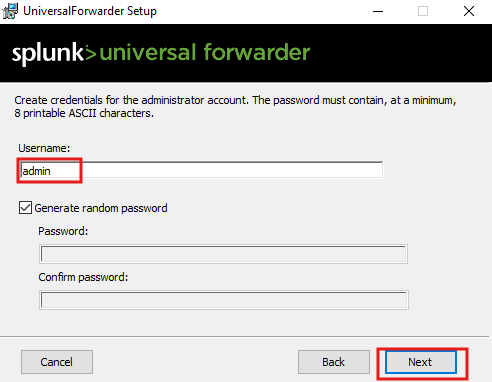
Once downloaded, double click on the .msi file to start installation.

Splunk Universal forwarder installation

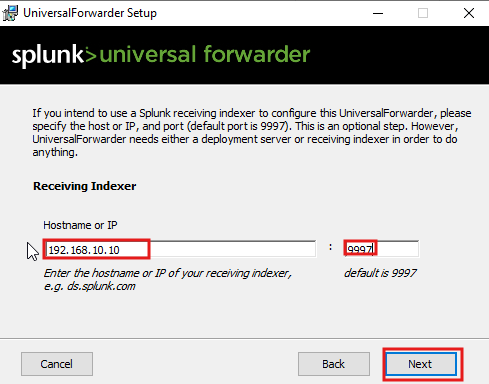
Then, accept the license agreement, check the on-premises option and click next.

Splunk Universal forwarder installation

Then, select a username and click next.

Splunk Universal forwarder installation

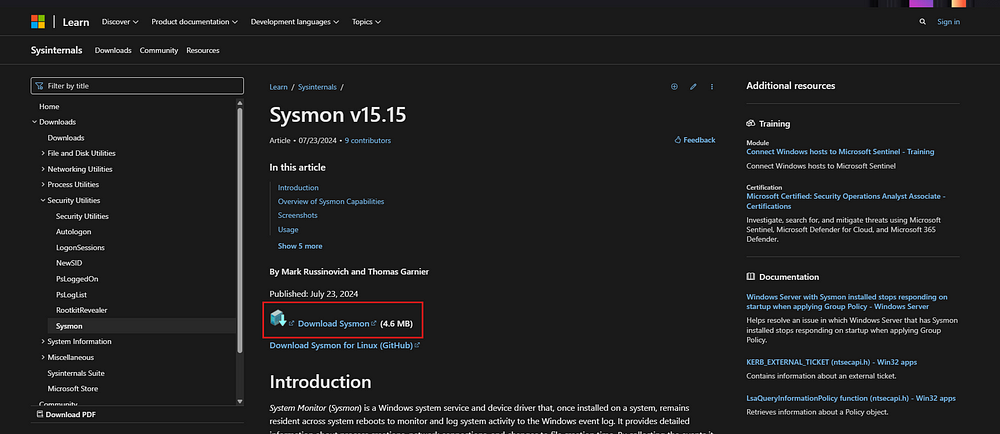
Then click next on the deployment server option, then give the Host Ip address as the ubuntu server address and the port as 9997 as this is the default listening port of Splunk.

Splunk Universal forwarder installation

Then click install.

**Sysmon Installation**

Download Sysmon installer from [here](https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon).

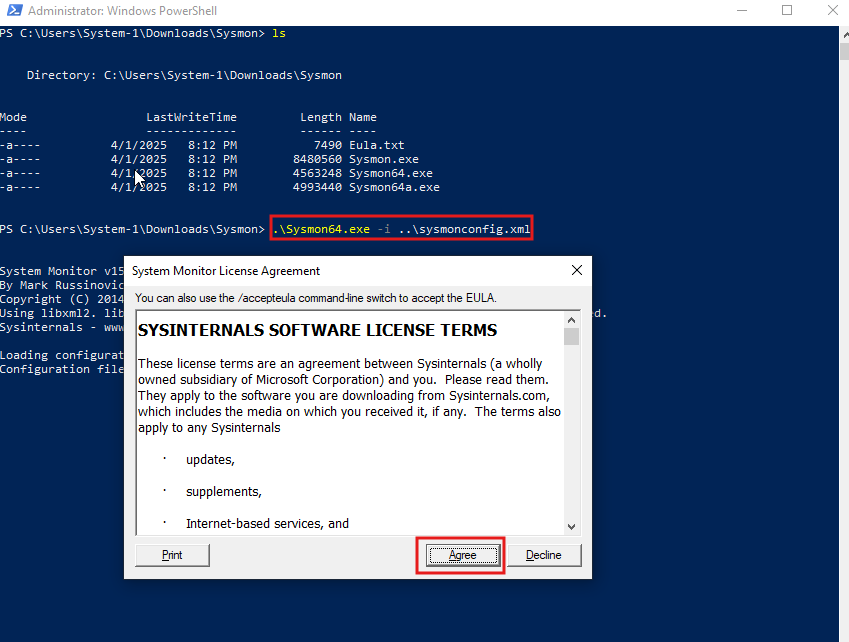
Sysmon download

Then download the configuration file required for Sysmon from here.

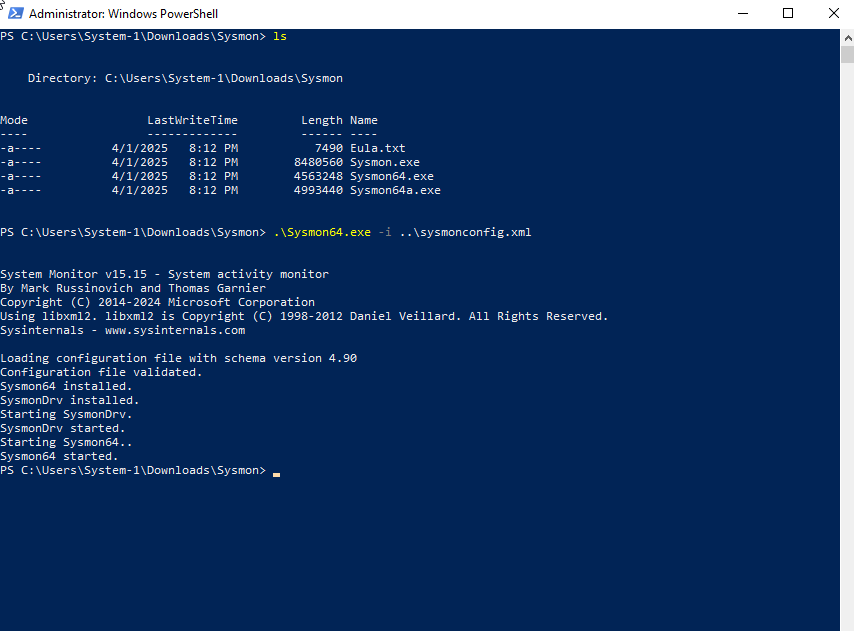
Sysmon config download

Now unzip the sysmon download and then open a powershell with admin privileges. Then navigate to the folder where Sysmon files are extracted and type the following command.

.\Sysmon.exe -i ..\sysmonconfig.xml

Sysmon installation

Now Sysmon will install and use the given configuration.

Sysmon installation

Now, we need to tell the splunk forwarder, what exactly it needs to forward. For this we can change the input.conf file under

C:\Program Files\SplunkUniversalForwarder\etc\System\default.

But to make sure that we can revert back to this configuration if something goes wrong, we will leave this untouched and create another file named inputs.conf under

C:\Program Files\SplunkUniversalForwarder\etc\System\local.

The file contains the following contents

[WinEventLog://Application]

index = endpoint

disabled = false

[WinEventLog://Security]

index = endpoint

disabled = false

[WinEventLog://System]

index = endpoint

disabled = false

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

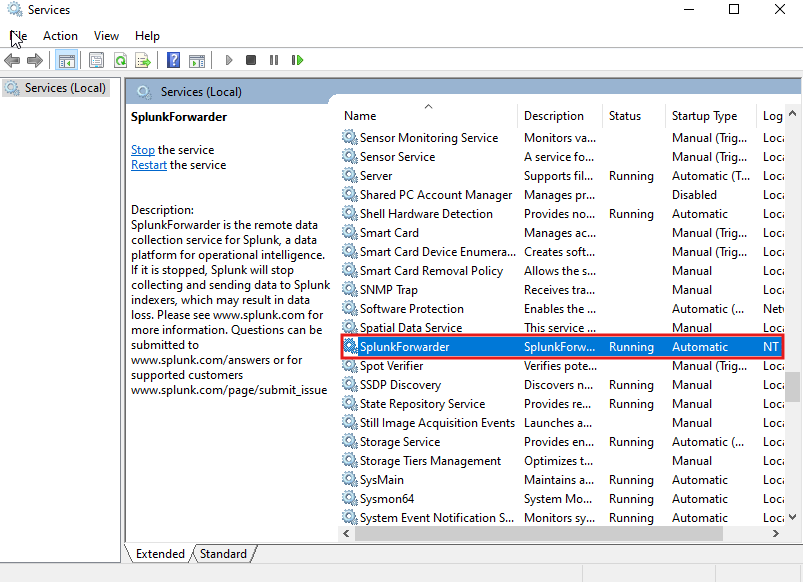
index = endpoint

disabled = false

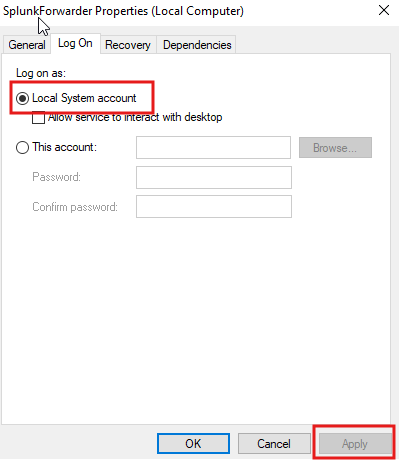
renderXml = true

source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

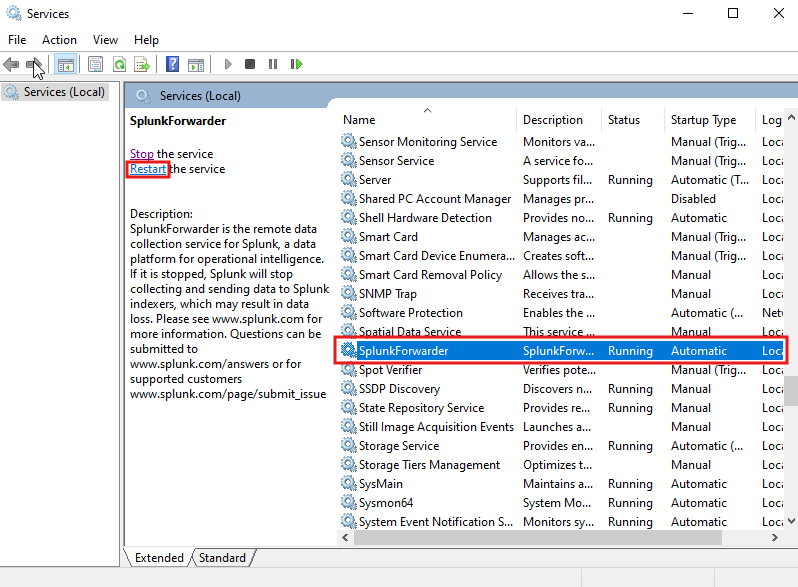
Inorder for the changes to take effect, we need to restart the splunk forwarder service. For this open service as admin and the double click on SplunkForwarder.



Now go to Log On section and select Local System account. Then click apply and ok.

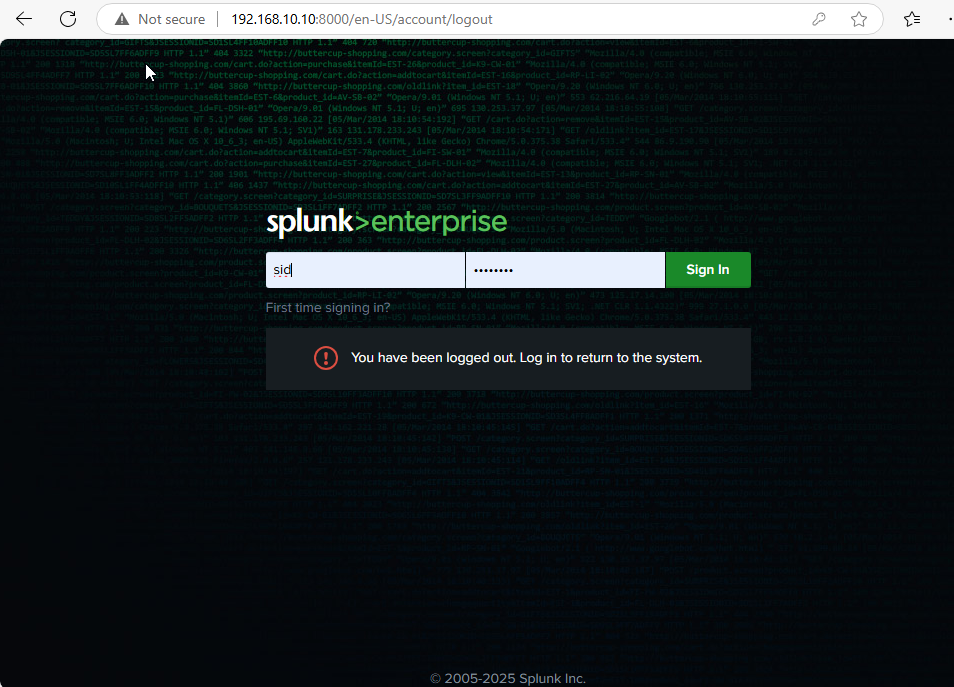


Now, under the services click on restart the service.

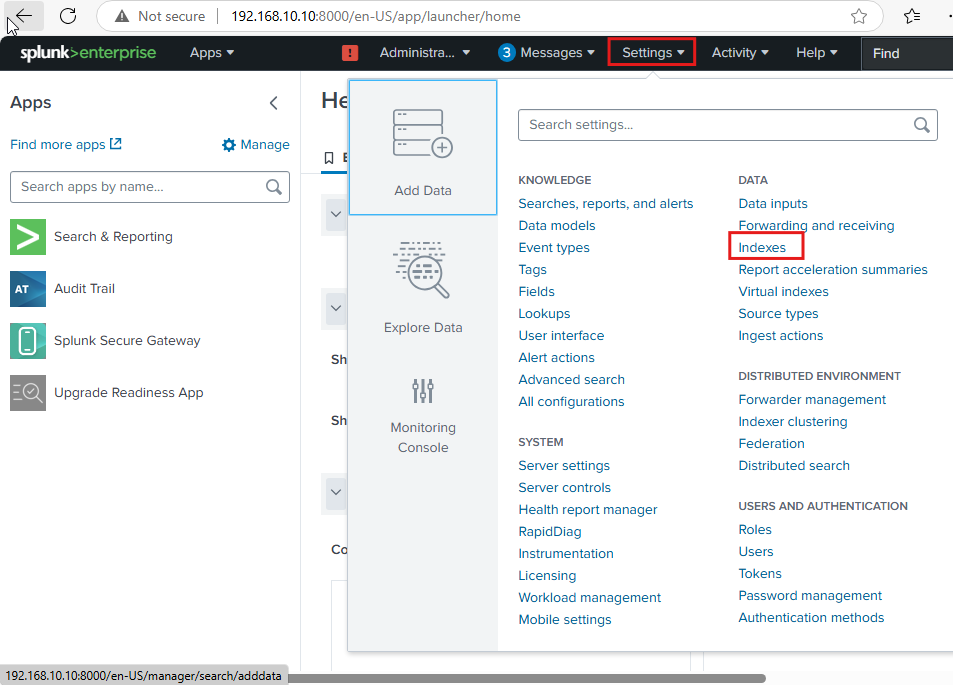


Now the SplunkForwarder and Sysmon are ready. **Following the similar steps we install the Splunk forwarder and Sysmon on our Windows Server**.

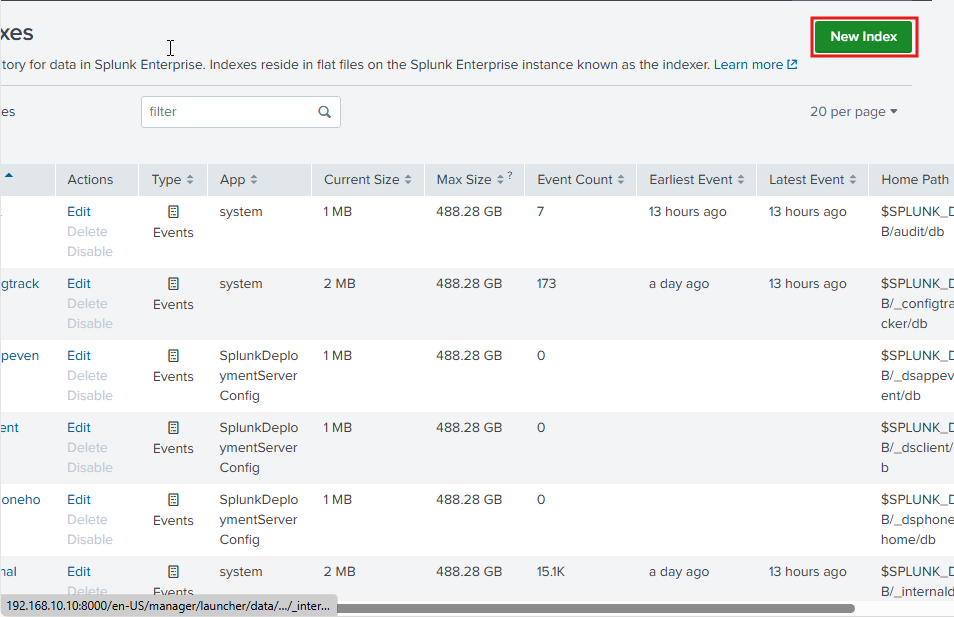
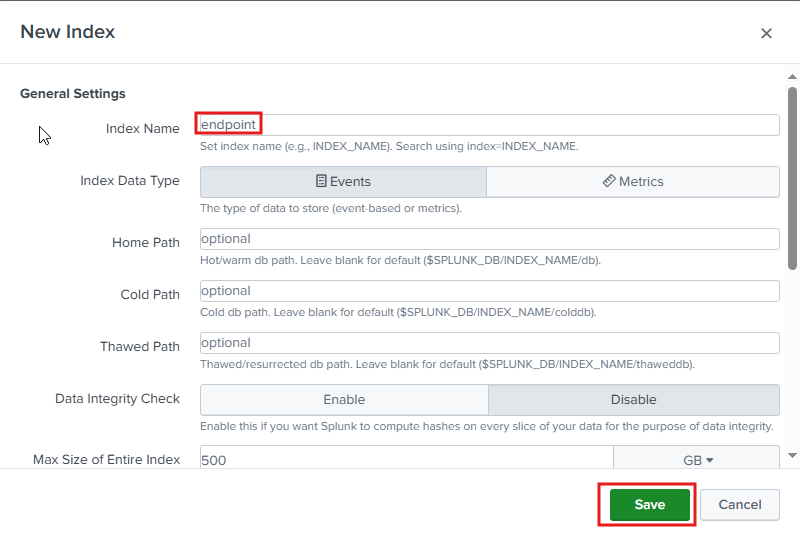
Now we can finalize the Splunk server configuration. Access the Splunk portal by navigating to 192.168.10.10:8000 in a browser on the windows VM. Then login using the credentials previously created while setting up Splunk.

Splunk Web portal

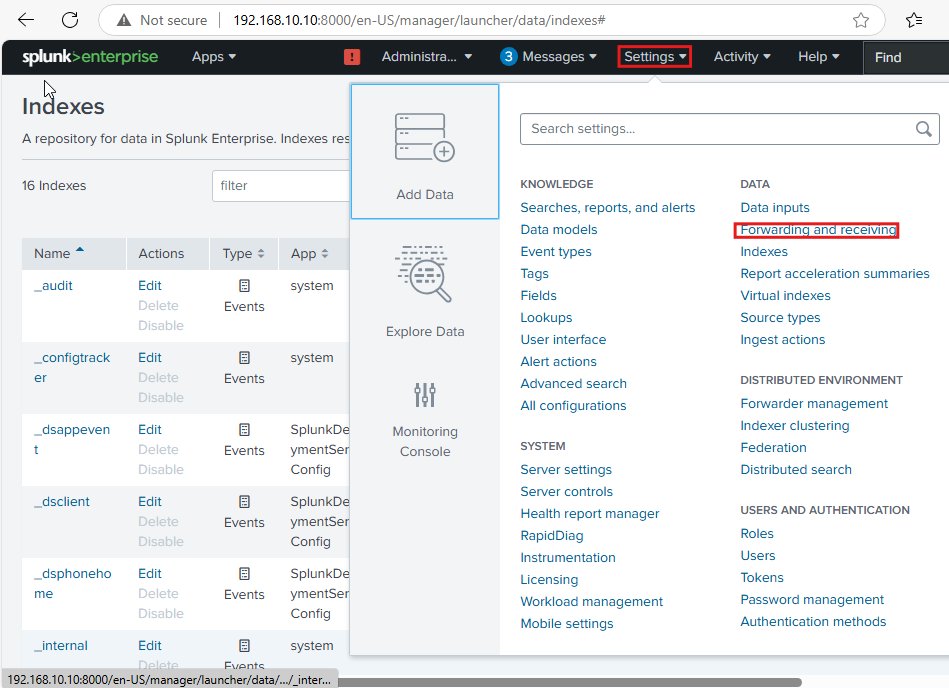
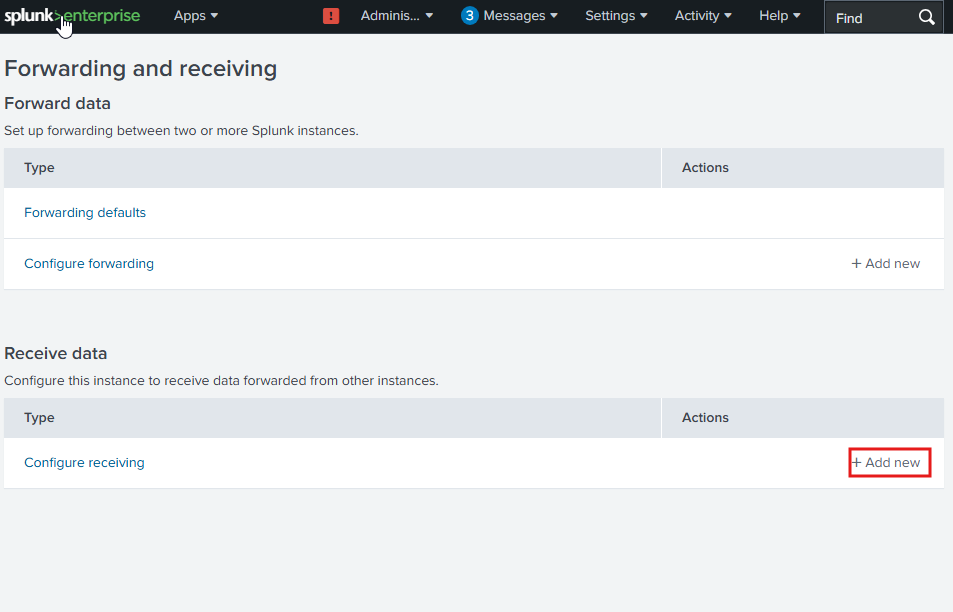
Once logged in, navigate to settings on the top and then click on indexes.

Splunk Web portal

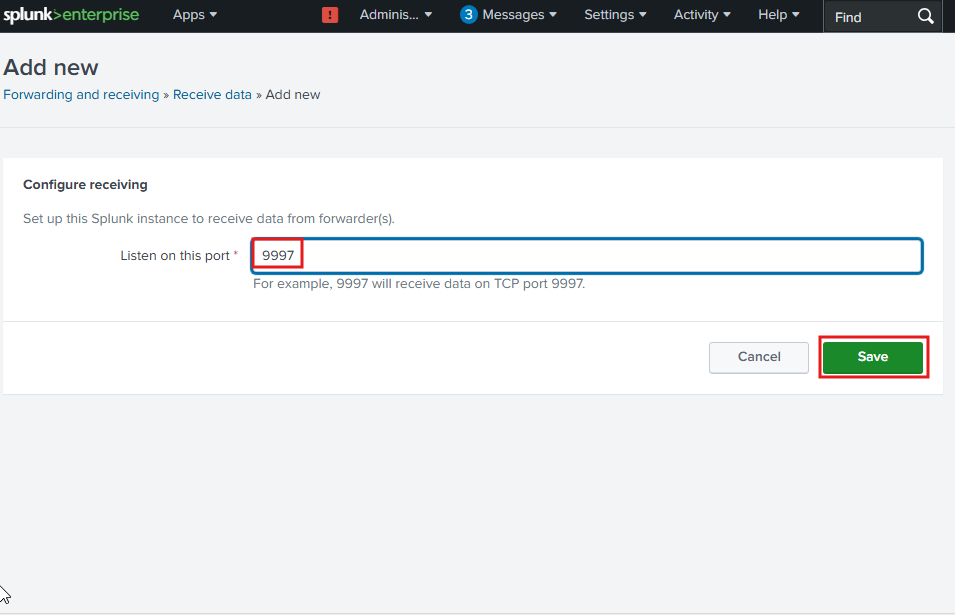
Here click on the New Index option on the top right and create an index named endpoint.

Splunk Web portalSplunk Web portal

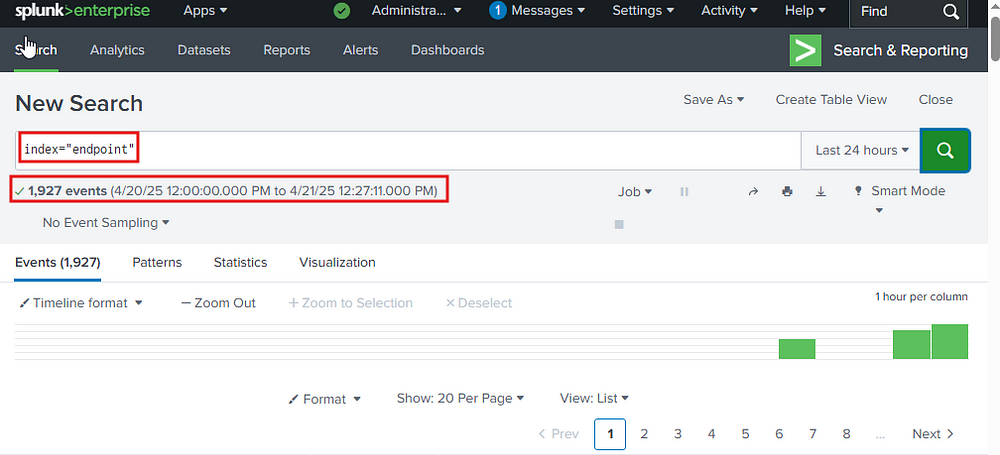
Once the index is created, we need to enable the Splunk server to receive the data. For this go to settings and Forwarding and Receiving. And under Receive data->Configure receiving click Add new.

Splunk Web portalSplunk Web portal

Under here, add the listening port and hit save.

Splunk Web portal

Once this is setup, we should start seeing data in our Splunk index. Go to the Search & Reporting app and search for index=”endpoint”.



As we can see above, we are receiving data from our endpoint.