Assignment :

✓ Integration of Splunk Enterprise and Universal Forwarder on Ubuntu System for Log Collection and Monitoring.

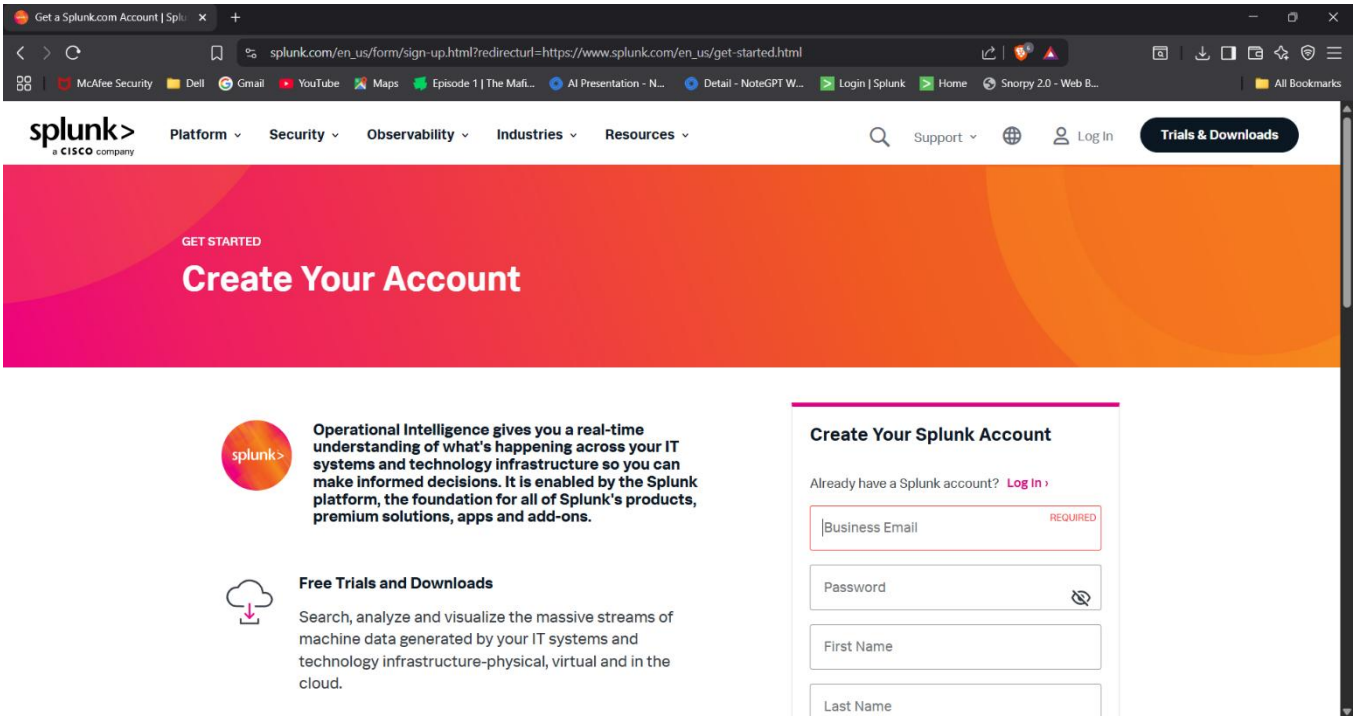
📌 **PROJECT CONTRIBUTOR:**

AJINKYA TAYADE

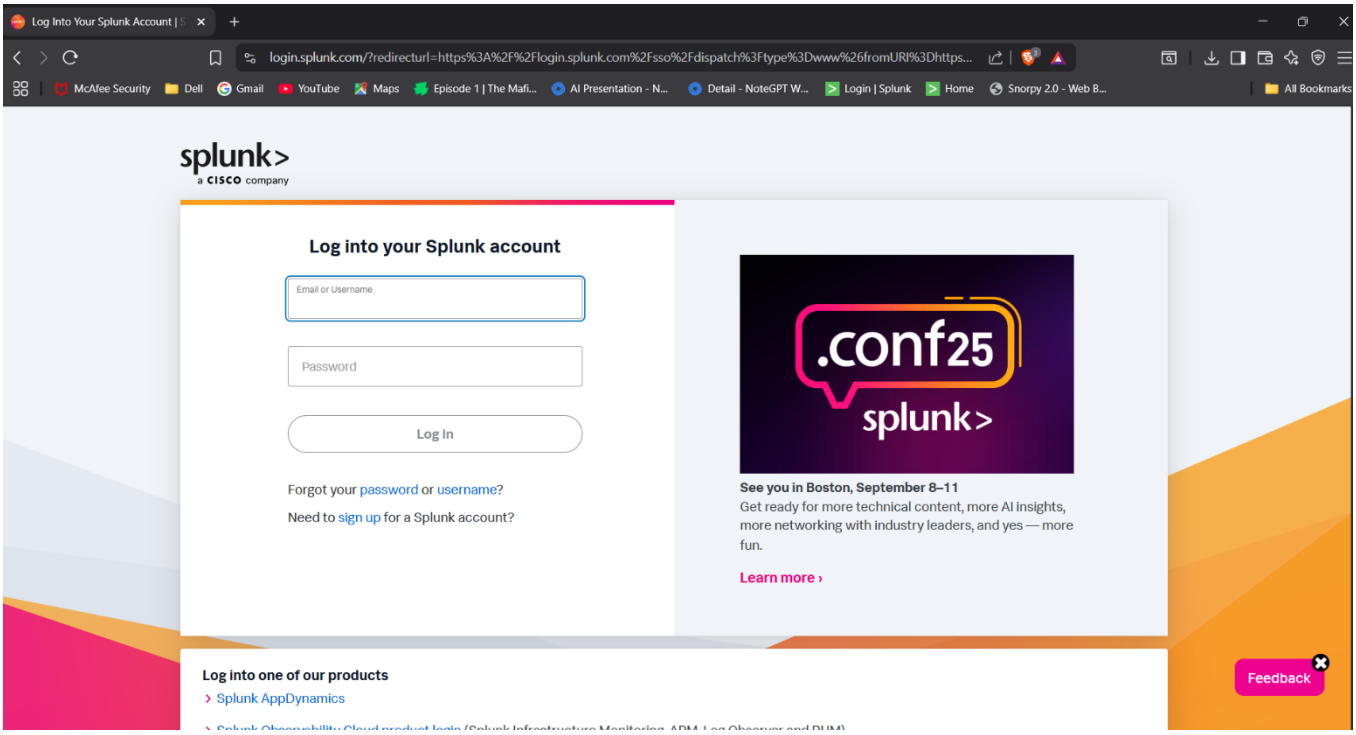
📧 ajinkyatayade43@gmail.com

- **Step 1:** Installation of Splunk® Enterprise Server

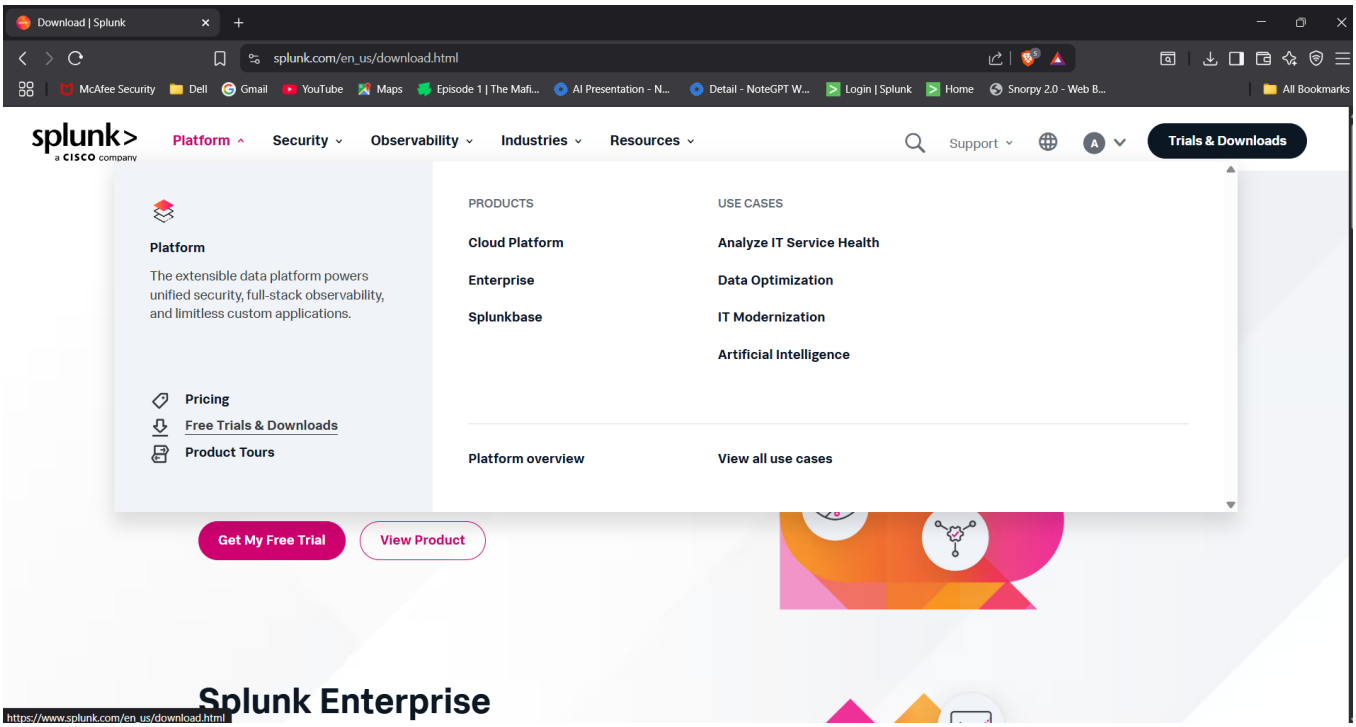
Splunk login/sing up link :
https://www.splunk.com/en_us/form/signup.html?redirecturl=https://www.splunk.com/



➡ Now login in Splunk account

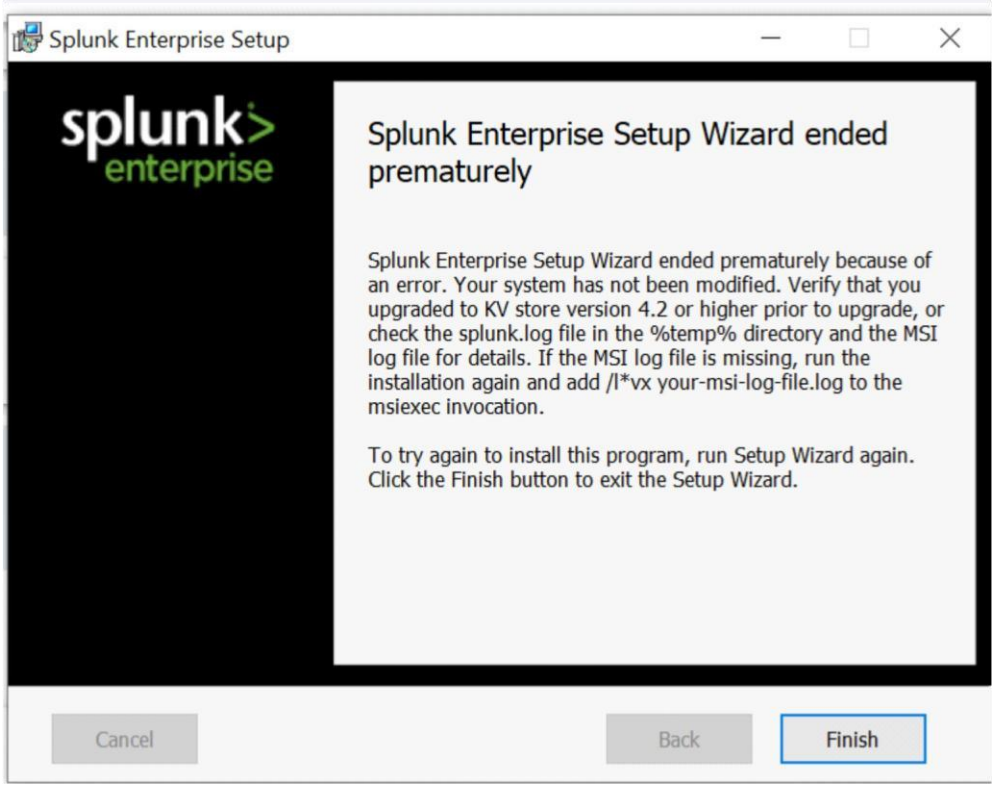


➡ Now go to platform and click on free trails and downloads



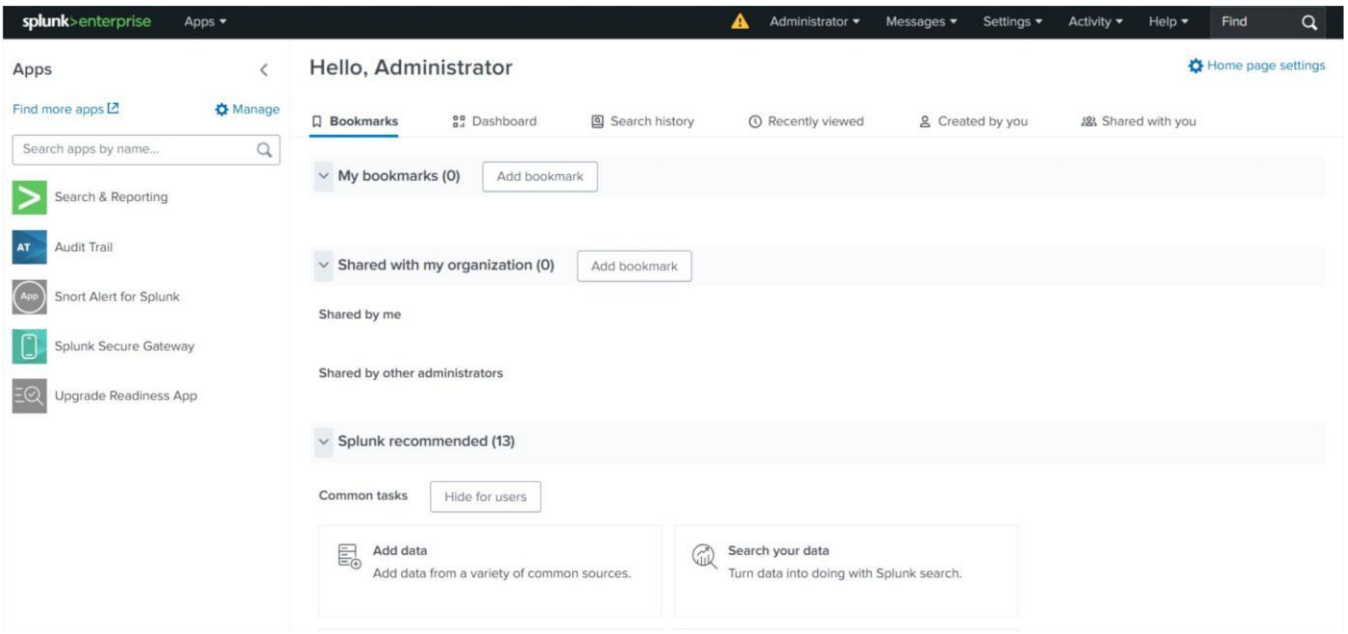
➡ After that need to install Splunk enterprise server for window as shown in below image

➡ **Install download package and create login credential for Splunk server**

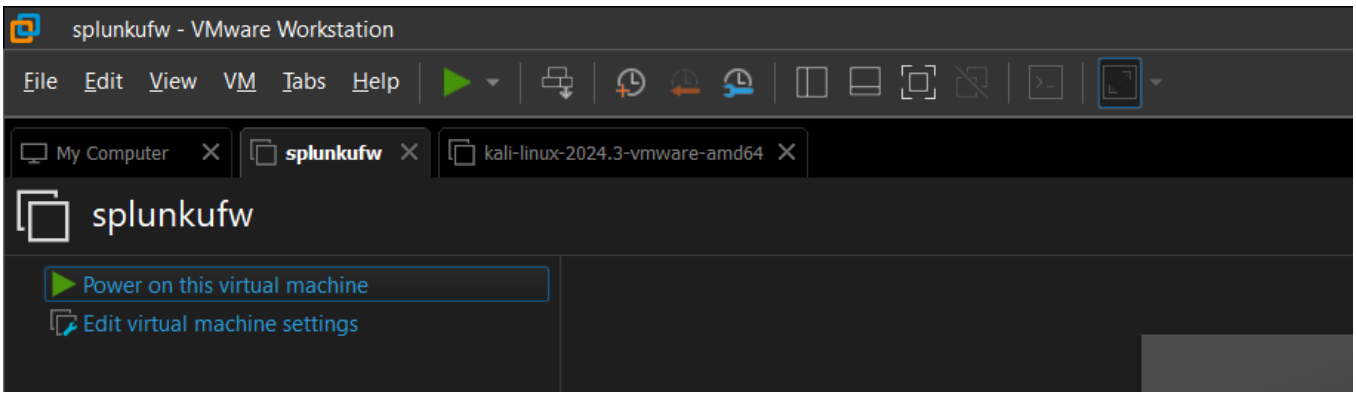


➡ **Now login into your Splunk enterprise server**

➡ **After that Dashboard of Splunk enterprise server appears like this,**



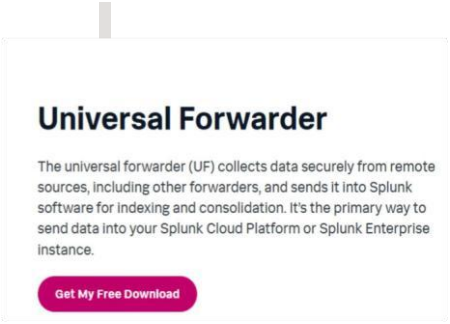
1Step 1: installation of Splunk Enterprise server is finished.

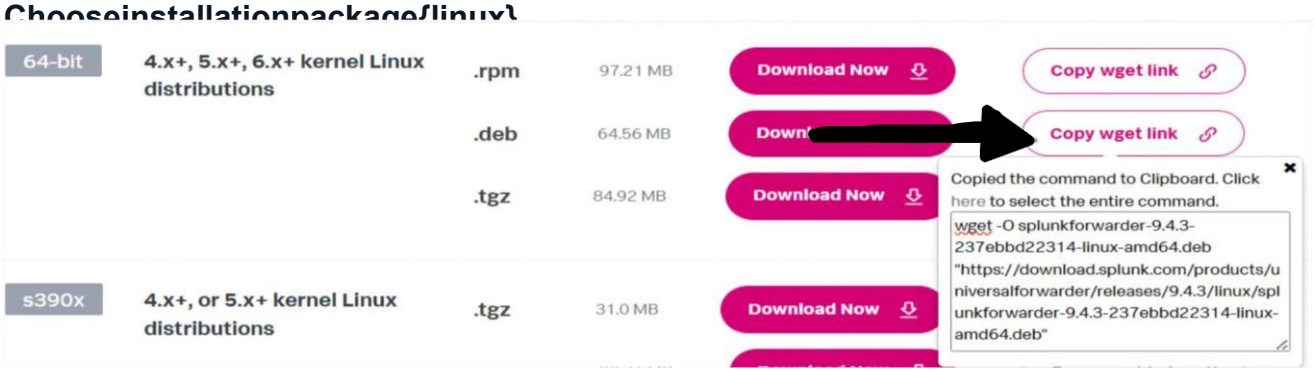


2 Step :- Install ubuntu server for forwarding logs to Splunk enterprise Server I'AM using VMware in I have installed ubuntu Server

After Successfully installation of ubuntu server get a link of forwarding server based on ubuntu server like Debian package follow same process for login in Splunk

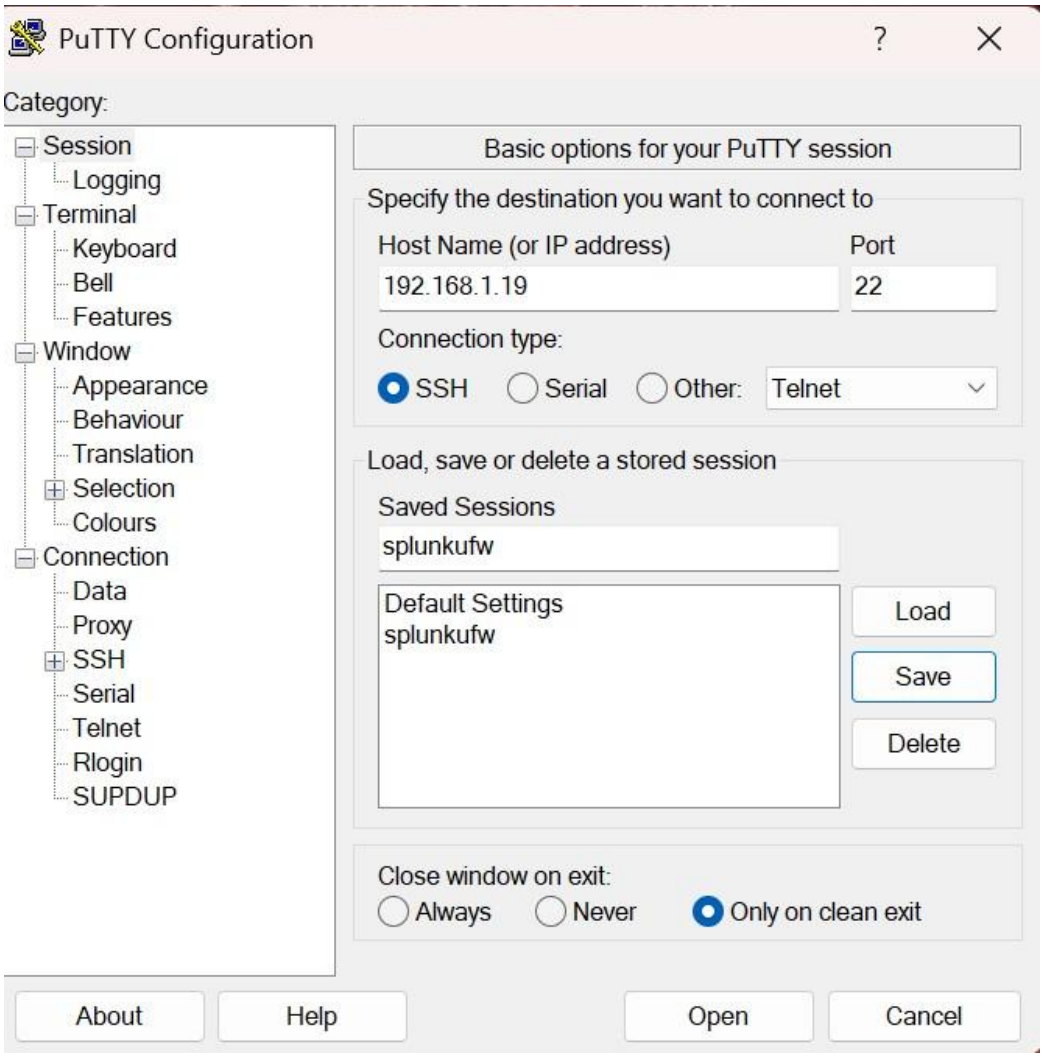
https://www.splunk.com/en_us/form/sign-up.html?redirecturl=https://www.splunk.com/ after that go to universal forwarder.



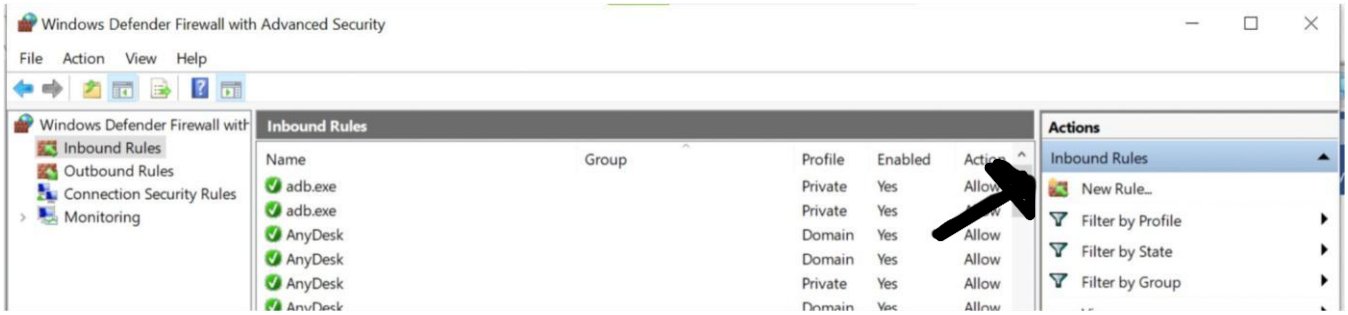


Copy wget link to install universal forwarder in ubuntu server save it into note pad for later.

After that make a connect between ubuntu serverand Putti using ssh.

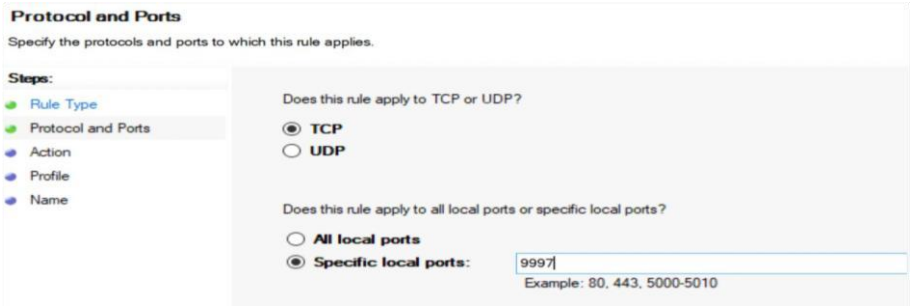


After established a connection successfully create a inbound rule in windows go to firewall & networks select Advance setting and create it as shown in screenshots below.

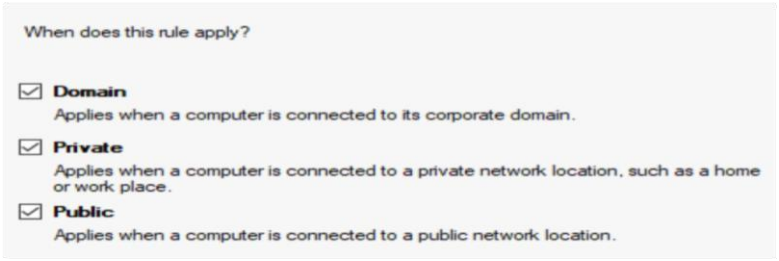


select a port and click on next

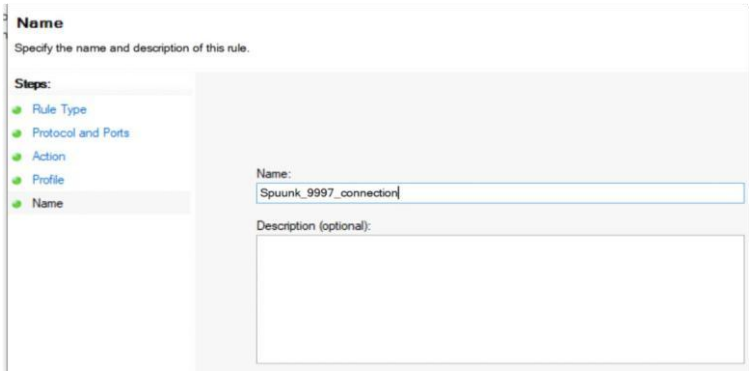
mention port no (9997) tcp and click on next



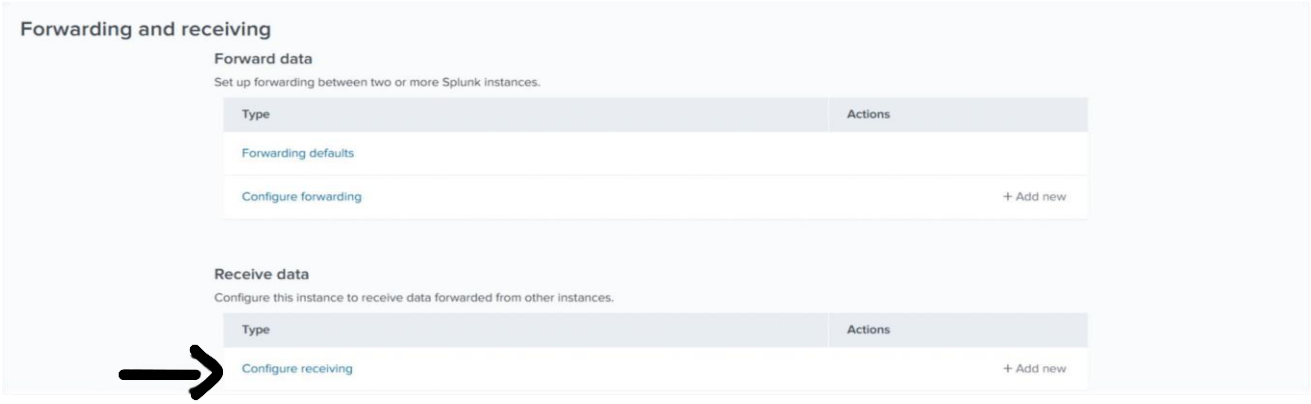
allow the connection and click on next

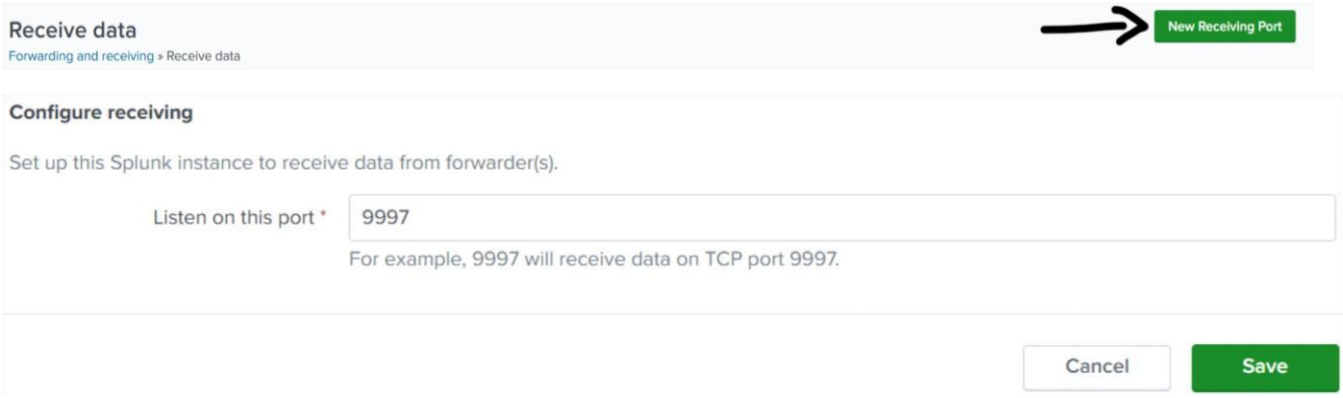


Then click on next and give a name to this connection



At the same time need to configure setting in Splunk enterprise server goto settings select forwarding and receiving after that click on configure receiving.





Configure receiving Setting listen to 9997 port and save it. Now inbound is successfully added to Splunk enterprise server.

Step 3 Installation of universal forwarder

As I have already copy universal forwarder wget link and make a ssh connection using putti.

#sudo ufw enable (allow firewall and active)

#sudo ufw allow 22/tcp (for tcp port 22 request)

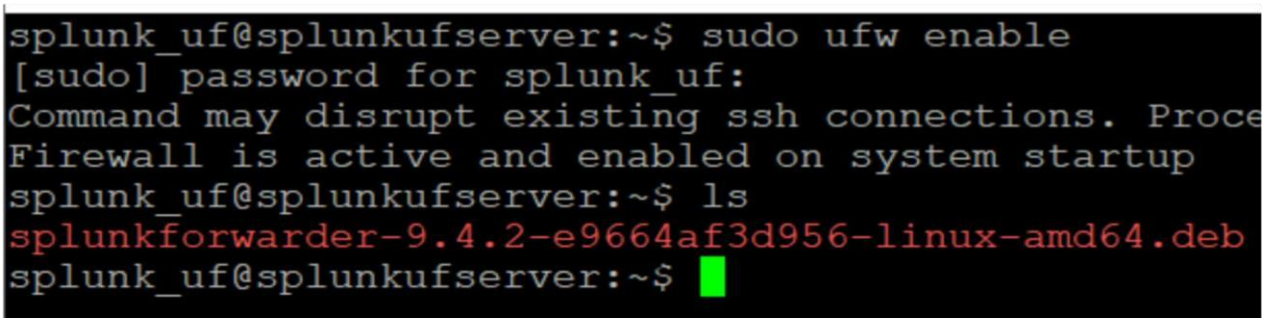
#sudo ufw allow 9997/tcp (for receiving port)

wget -O splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/splunkforwarder-9.4.3237ebbd22314-linux-amd64.deb (for installation of universal forwarder)

After that we can see package and for installation this apagoge use this command #sudo

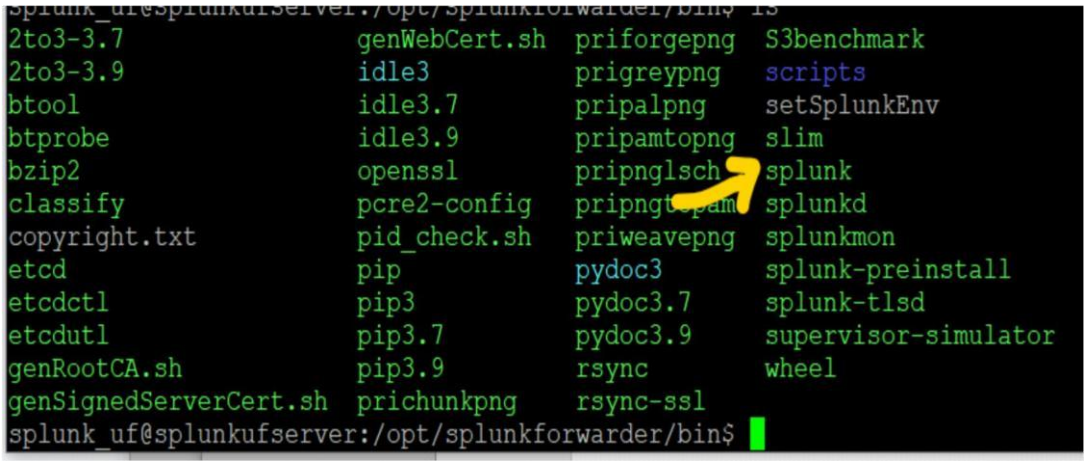
dpkg -I splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb (package name) Press

Enter, Please wait,as this may take a few minutes.



For run a Splunk forwarder follow this path

ls (for list of file and directories)



Now its time time connect splunk forwarder to Splunk Enterprise server using below command

#sudo ./splunk add forward-server 192.168.xx.xx:9997 -auth admin:admin (Splunk enterprise ip along with port no 9997)

Asking foe license press y/yes and press Enter.

(Splunk enterprise server added successfully)

Restart Splunk

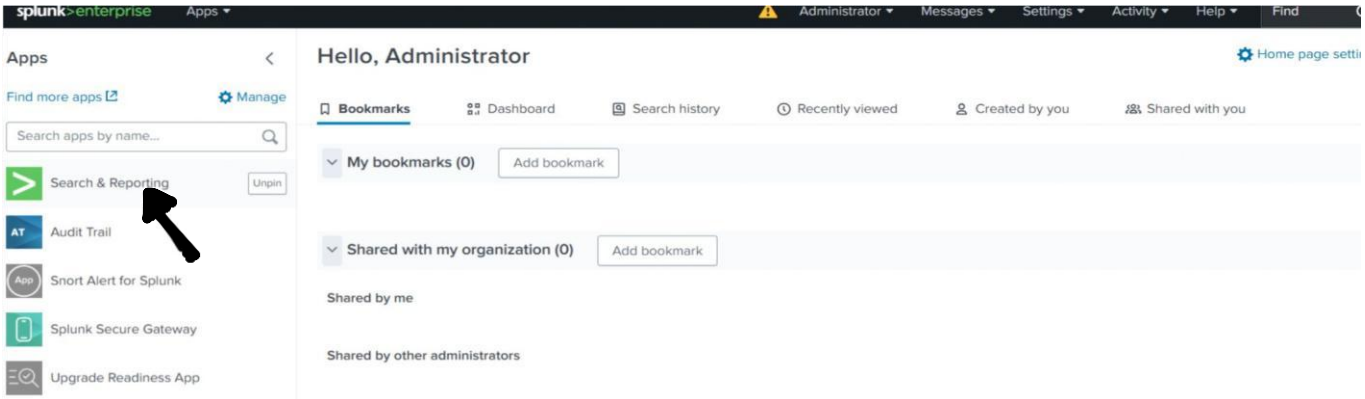
#sudo ./splunk restart

Step 2 after added server

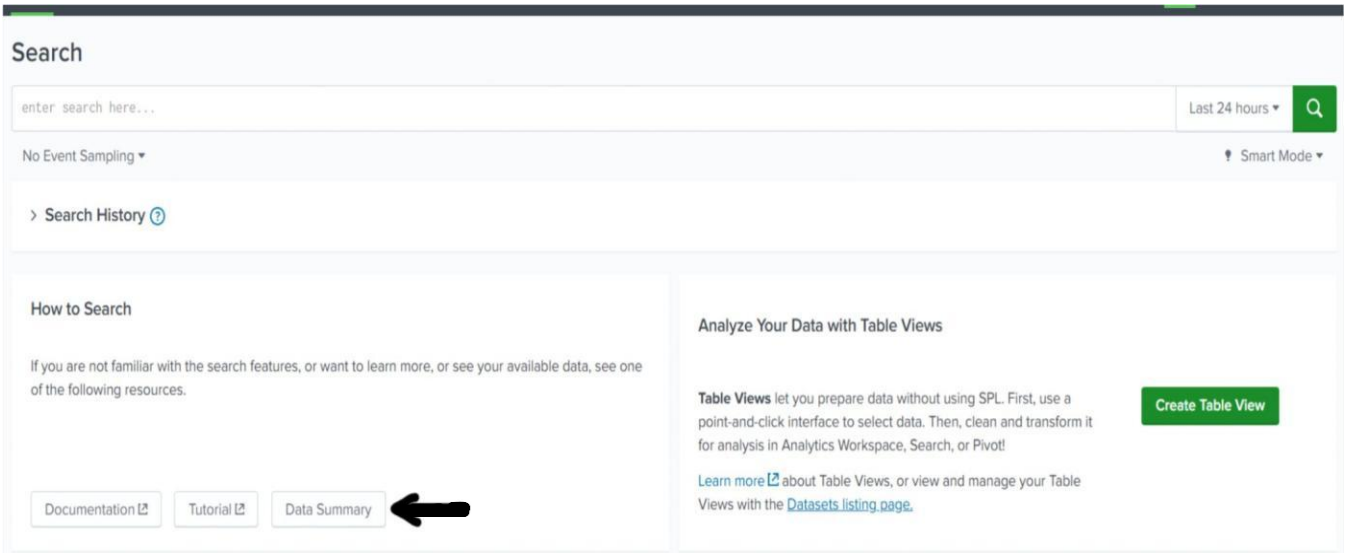
sudo ./splunk add monitor /var/log

sudo ./splunk add monitor /var/log/auth.log -auth admin:admin (logs / files which have o be monitor is added using this command)

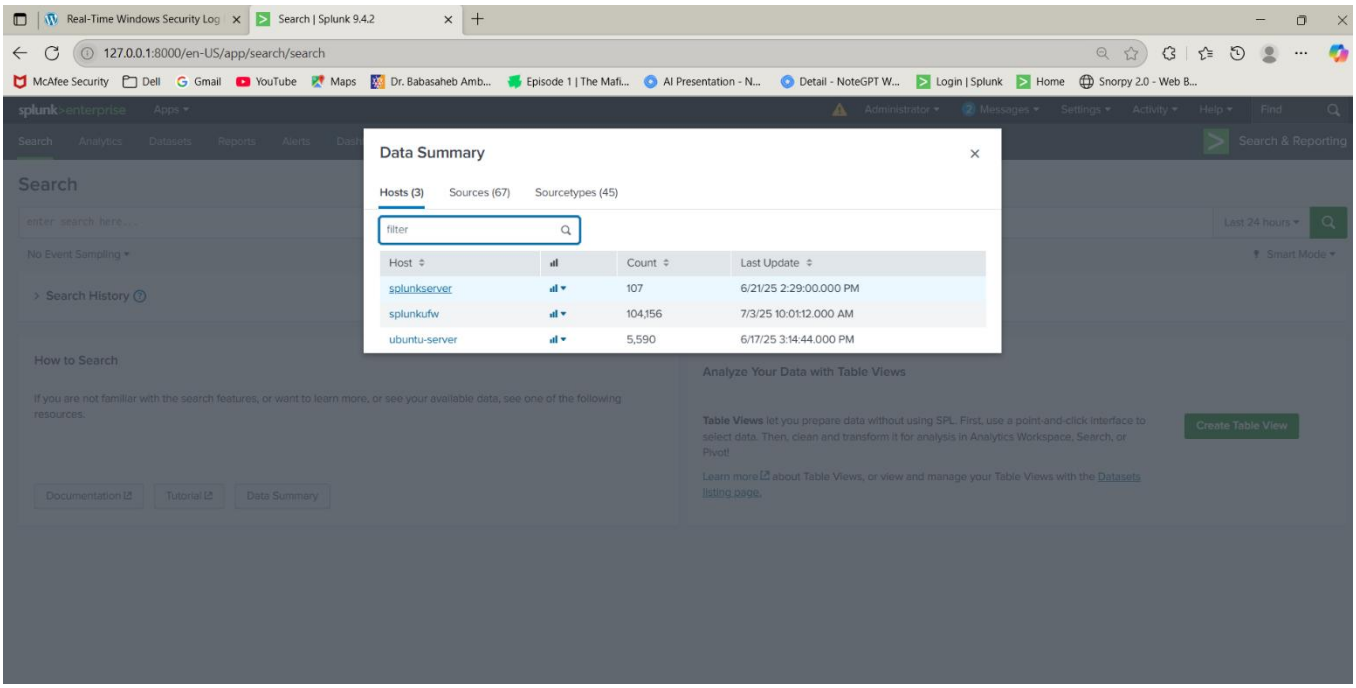
Go to Splunk enterprise server and select search and report.



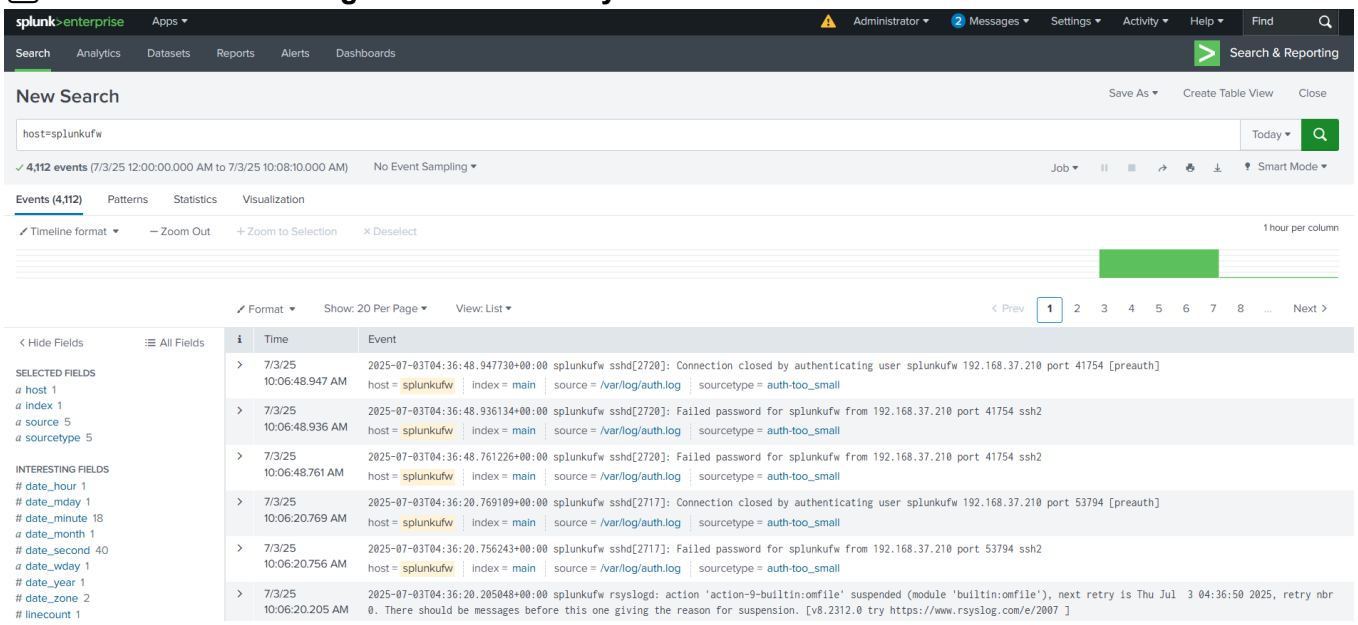
➡️ **Click on data Summary**



🌓 **Click on Hosts ,**



➡️ Now able to see all logs which is send by universal forwarder.



✓ Summary:

This setup demonstrates the successful deployment of Splunk® Enterprise and Universal Forwarder on Ubuntu, enabling efficient log forwarding and centralized monitoring.

It provides a strong foundation for:

🔐 Security Analysis

🌓 System Auditing

📊 Real-Time Log Management

This implementation helps organizations maintain visibility into system activities and ensures better incident detection and response.