

## Assignment :

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

#### PROJECT CONTRIBUTOR:

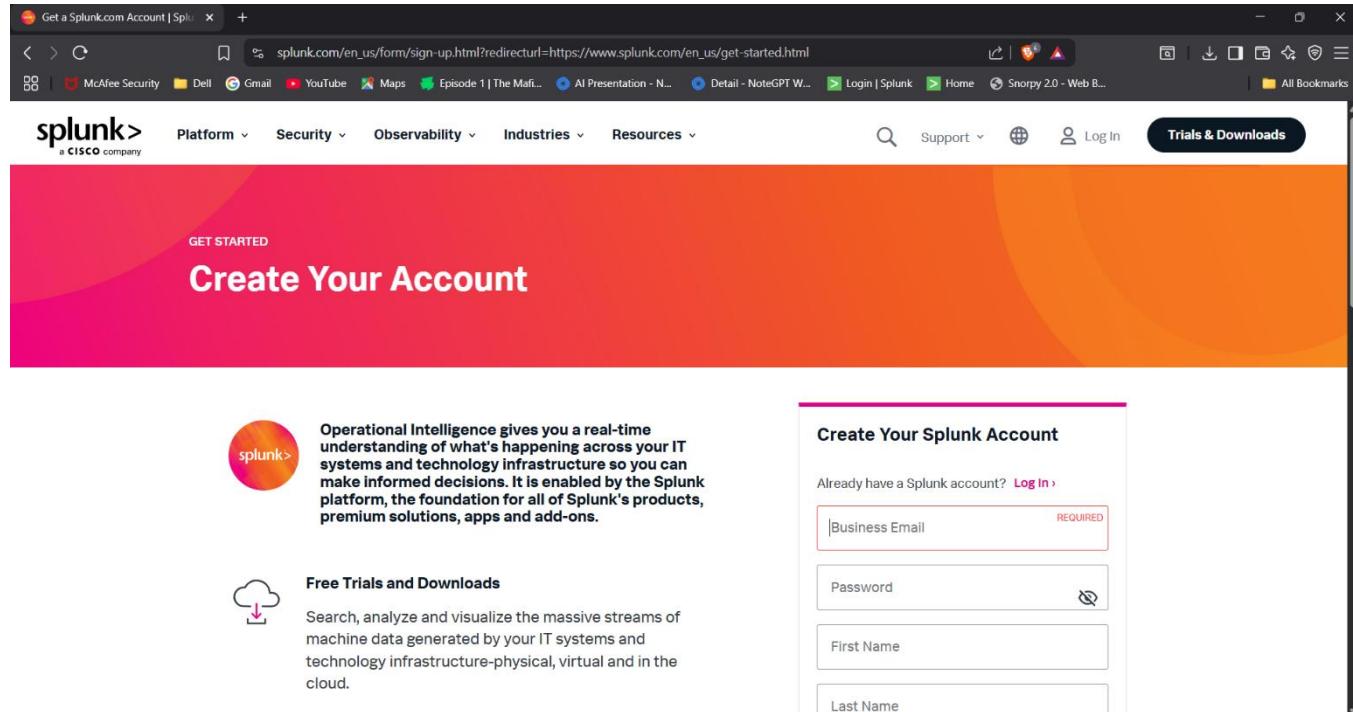
AJINKYA TAYADE

 ajinkyatayade43@gmail.com

#### ◊ Step 1: Installation of Splunk® Enterprise Server

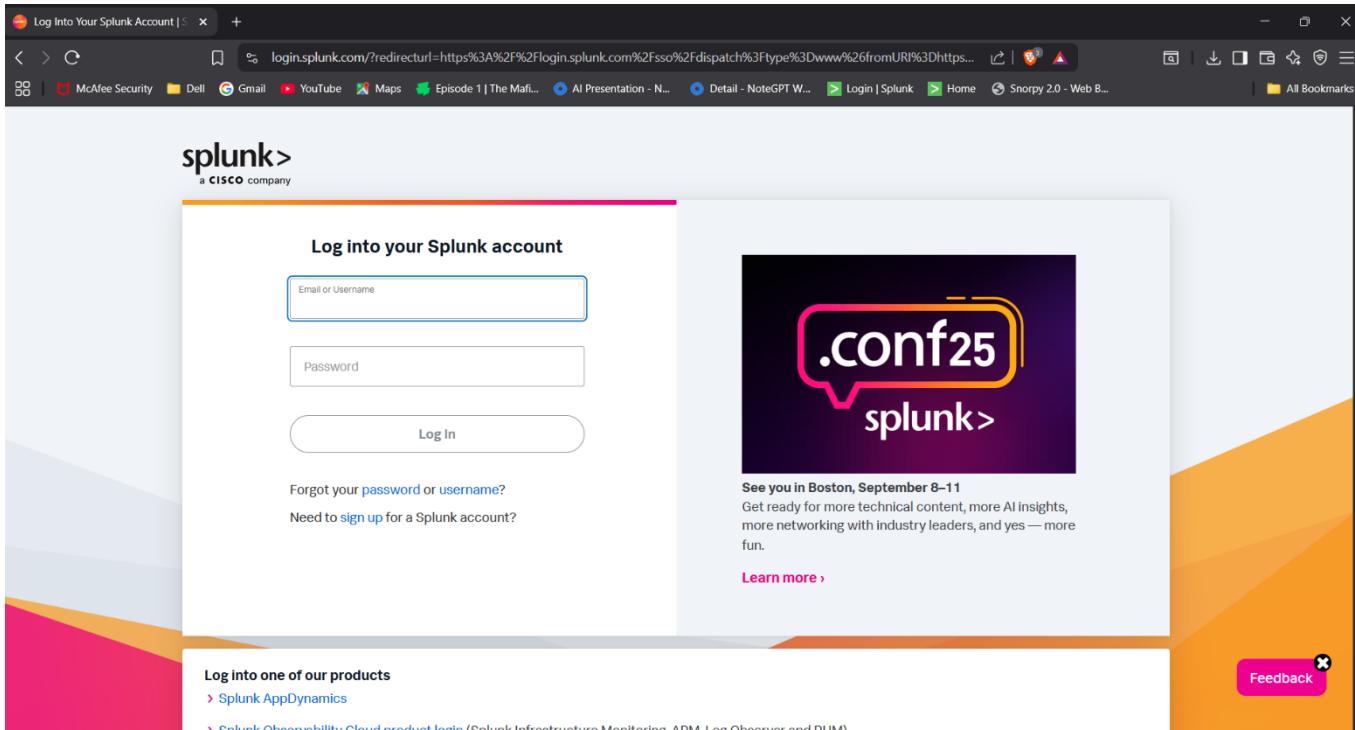
Splunk login/sing up link :

[https://www.splunk.com/en\\_us/form/signup.html?redirecturl=https://www.splunk.com/](https://www.splunk.com/en_us/form/signup.html?redirecturl=https://www.splunk.com/)

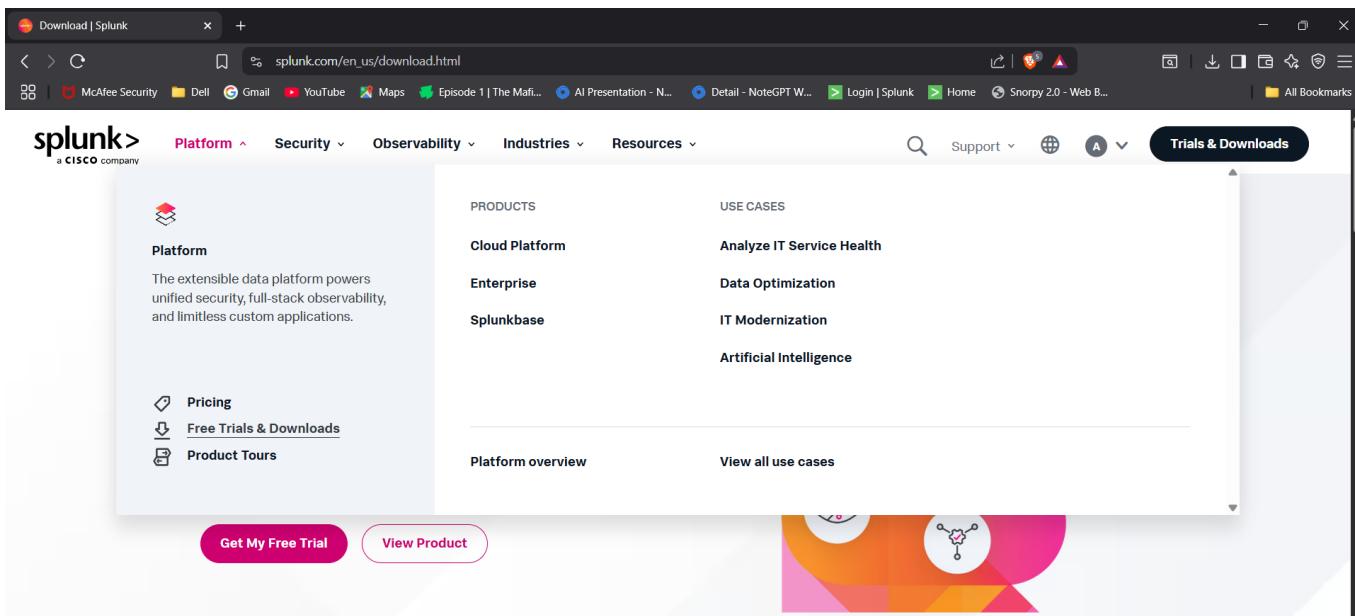


The screenshot shows a web browser window with the URL [splunk.com/en\\_us/form/signup.html?redirecturl=https://www.splunk.com/](https://www.splunk.com/en_us/form/signup.html?redirecturl=https://www.splunk.com/). The page has a red-to-orange gradient background. At the top, there's a navigation bar with links for Platform, Security, Observability, Industries, and Resources. On the right side of the header, there are links for Support, Log In, and Trials & Downloads. Below the header, a large button says "Create Your Account". To the left of the form, there's a circular "splunk>" logo and some descriptive text about operational intelligence. The main form area is titled "Create Your Splunk Account" and contains fields for Business Email, Password, First Name, and Last Name. There are also links for "Free Trials and Downloads" and "Already have a Splunk account? Log In".

## ➡ Now login in Splunk account



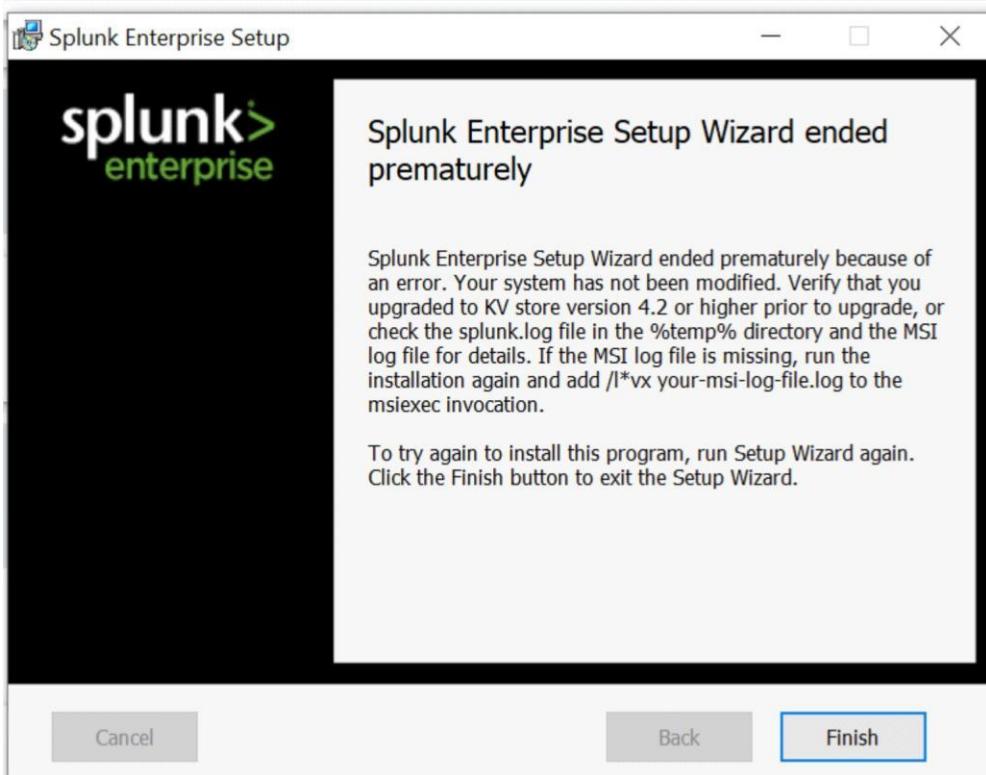
## ➡ Now go to platform and click on free trials and downloads



## Splunk Enterprise

➡ 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



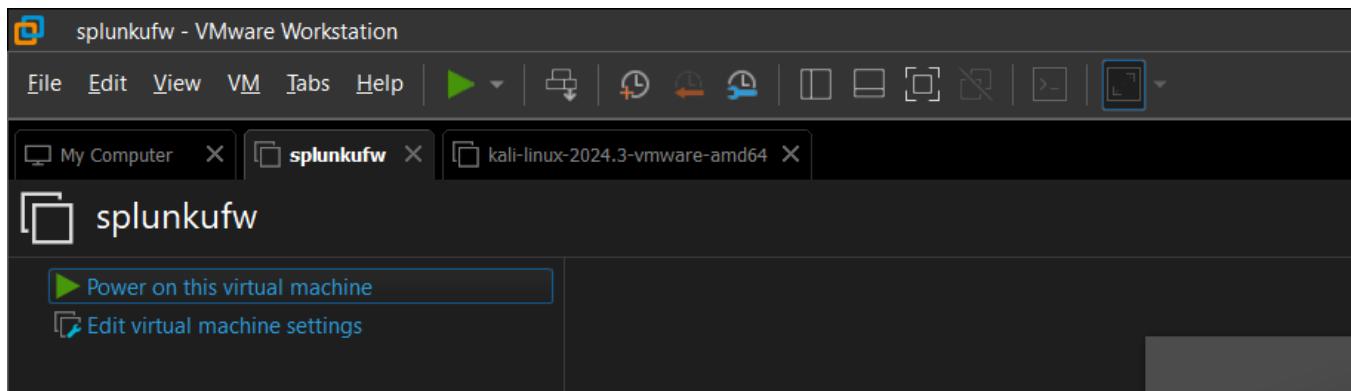
➡ Now login into your Splunk enterprise server



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

The screenshot shows the Splunk Enterprise dashboard. On the left, there's a sidebar titled 'Apps' with icons for 'Search & Reporting', 'Audit Trail', 'Snort Alert for Splunk', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. The main area is titled 'Hello, Administrator'. It features a 'Bookmarks' section with 'My bookmarks (0)', 'Shared with my organization (0)', and 'Splunk recommended (13)'. Below this are 'Common tasks' like 'Add data' and 'Search your data'.

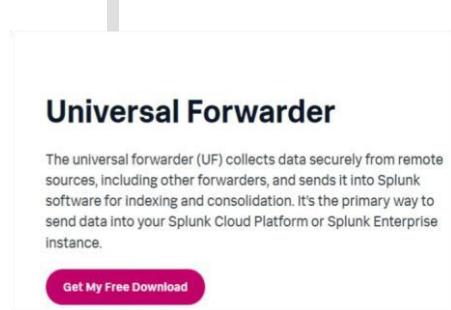
## 1 Step 1: Installation of Splunk Enterprise server is finished.



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



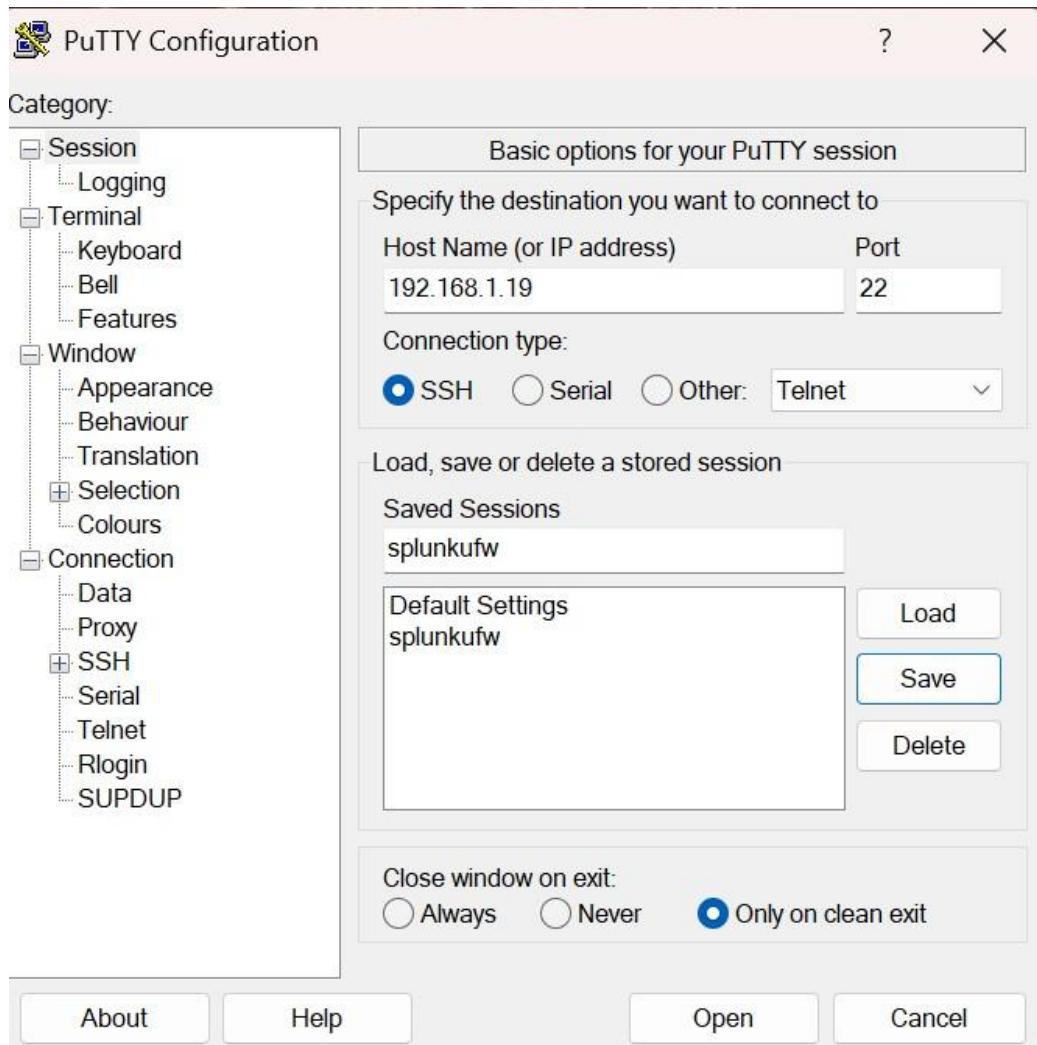
#### Choose installation package for Linux

64-bit	4.x+, 5.x+, 6.x+ kernel Linux distributions	.rpm	97.21 MB	Download Now	Copy wget link
		.deb	64.56 MB	Download Now	Copy wget link
		.tgz	84.92 MB	Download Now	Copy wget link
s390x	4.x+, or 5.x+ kernel Linux distributions	.tgz	31.0 MB	Download Now	Copy wget link

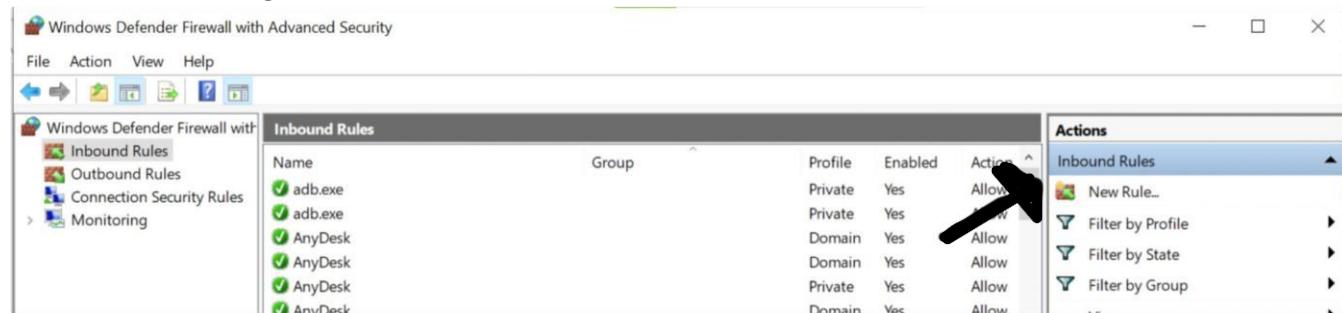
A screenshot showing the download options for the Splunk Universal Forwarder. For the 64-bit section, there are three rows: one for .rpm (97.21 MB), one for .deb (64.56 MB), and one for .tgz (84.92 MB). Each row has a 'Download Now' button and a 'Copy wget link' button. An arrow points from the 'Copy wget link' button for the .deb row to a tooltip. The tooltip contains the command: 'Copied the command to Clipboard. Click here to select the entire command.' followed by the wget command: 'wget -O splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb"'.

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

After that make a connect between ubuntu server and 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

#### Protocol and Ports

Specify the protocols and ports to which this rule applies.

##### Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

- TCP
- UDP

Does this rule apply to all local ports or specific local ports?

- All local ports
- Specific local ports:

9997

Example: 80, 443, 5000-5010

allow the connection and click on next

When does this rule apply?

Domain

Applies when a computer is connected to its corporate domain.

Private

Applies when a computer is connected to a private network location, such as a home or work place.

Public

Applies when a computer is connected to a public network location.

Then click on next and give a name to this connection

#### Name

Specify the name and description of this rule.

##### Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:

Spuunk\_9997\_connection

Description (optional):

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

#### Forwarding and receiving

##### Forward data

Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

##### Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new



The screenshot shows the 'Receive data' configuration page in Splunk. At the top right is a large green arrow pointing to the right, with the text 'New Receiving Port' next to it. Below the arrow is a 'Cancel' button and a green 'Save' button. In the center, there's a section titled 'Configure receiving' with the sub-instruction 'Set up this Splunk instance to receive data from forwarder(s.)'. A field labeled 'Listen on this port \*' contains the value '9997'. Below this field is a note: 'For example, 9997 will receive data on TCP port 9997.' At the bottom of the page are two buttons: 'Cancel' and 'Save'.

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.

```
splunk_uf@splunkufserver:~$ sudo ufw enable
[sudo] password for splunk_uf:
Command may disrupt existing ssh connections. Proceed with caution!
Firewall is active and enabled on system startup
splunk_uf@splunkufserver:~$ ls
splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb
splunk_uf@splunkufserver:~$
```

For run a Splunk forwarder follow this path

```
splunk_uf@splunkufserver:~$ cd /opt/splunkforwarder/bin
# ls (for list of file and directories)
```

```

splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ ls
2to3-3.7          genWebCert.sh  priforgetpng  S3benchmark
2to3-3.9          idle3         prigreypng  scripts
btool             idle3.7       pripalpng   setSplunkEnv
btprobe            idle3.9       pripamtopng slim
bzip2              openssl       pripnglsch  splunk
classify           pcre2-config  pripngtopam splunkd
copyright.txt     pid_check.sh priweavepng splunkmon
etcd               pip           pydoc3      splunk-preinstall
etcdctl            pip3          pydoc3.7    splunk-tlsd
etcdutl            pip3.7       pydoc3.9    supervisor-simulator
genRootCA.sh       pip3.9       rsync       wheel
genSignedServerCert.sh prichunkpng rsync-ssl
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ 

```

Now its time to 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 for license press y/yes and press Enter.

```

[sudo] password for splunk:
Added forwarding to: 192.168.1.1:9997.

```

(Splunk enterprise server added successfully)

Restart Splunk

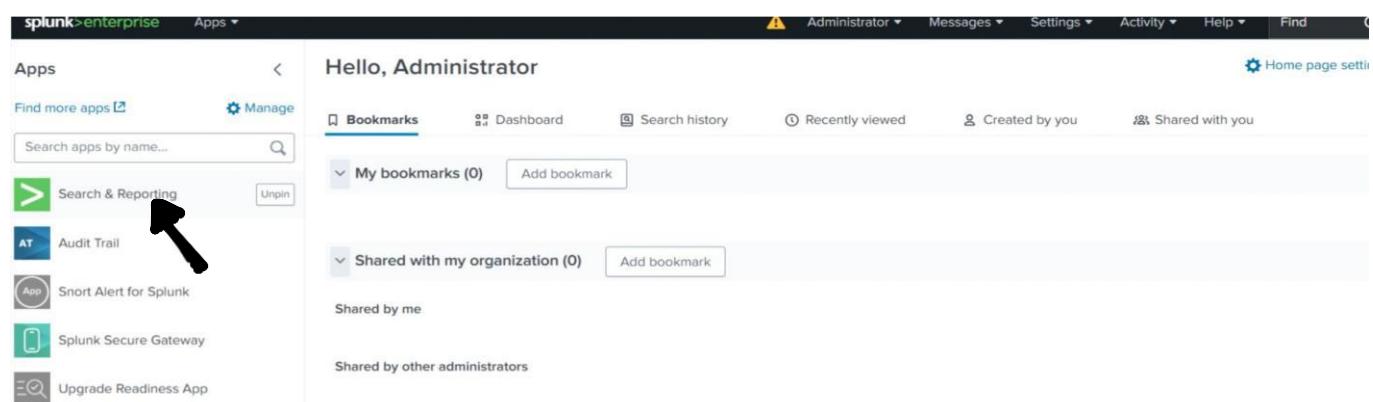
```
#sudo ./splunk restart
```

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 to be monitored are added using this command)
```

Go to Splunk enterprise server and select search and report.



➡ Click on data Summary

The screenshot shows the Splunk search interface. At the top, there is a search bar with the placeholder "enter search here...". To the right of the search bar are buttons for "Last 24 hours" and a magnifying glass icon. Below the search bar, there is a dropdown menu set to "No Event Sampling" and a "Smart Mode" toggle. A link to "Search History" is also present. On the left, there is a "How to Search" section with a paragraph of text and three buttons: "Documentation", "Tutorial", and "Data Summary". An arrow points to the "Data Summary" button. On the right, there is a section titled "Analyze Your Data with Table Views" containing text about Table Views, a "Create Table View" button, and a link to the "Datasets listing page".

⌚ Click on Hosts ,

The screenshot shows the Splunk search interface with the "Data Summary" tab selected. The main area displays a table titled "Hosts (3)" with columns for "Host", "Count", and "Last Update". The table contains three rows: "splunkserver" (Count: 107, Last Update: 6/21/25 2:29:00.000 PM), "splunkufw" (Count: 104,156, Last Update: 7/3/25 10:01:12.000 AM), and "ubuntu-server" (Count: 5,590, Last Update: 6/17/25 3:14:44.000 PM). The interface includes a search bar at the top, a navigation bar with links like "Search", "Analytics", "Datasets", etc., and a "How to Search" section with a paragraph of text and three buttons: "Documentation", "Tutorial", and "Data Summary". On the right, there is a section titled "Analyze Your Data with Table Views" containing text about Table Views, a "Create Table View" button, and a link to the "Datasets listing page".

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

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with 'splunk>enterprise' and various links like 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right of the top bar are 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the top bar is a search bar containing 'host=splunkufw'. To the right of the search bar are buttons for 'Save As', 'Create Table View', and 'Close'. The main area is titled 'New Search' and contains a search bar with the query 'host=splunkufw'. Below it, it says '✓ 4,112 events (7/3/25 12:00:00.000 AM to 7/3/25 10:08:10.000 AM) No Event Sampling'. There are tabs for 'Events (4,112)', 'Patterns', 'Statistics', and 'Visualization'. Under 'Events', there are buttons for 'Timeline format', 'Zoom Out', 'Zoom to Selection', and 'Deselect'. A green progress bar at the bottom indicates '1 hour per column'. The results table has columns for 'Time' and 'Event'. It lists several log entries from 'splunkufw' host, including failed SSH logins and a message about a suspended action. The table includes a header for 'Selected Fields' and 'Interesting Fields'.

### ✓ 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.