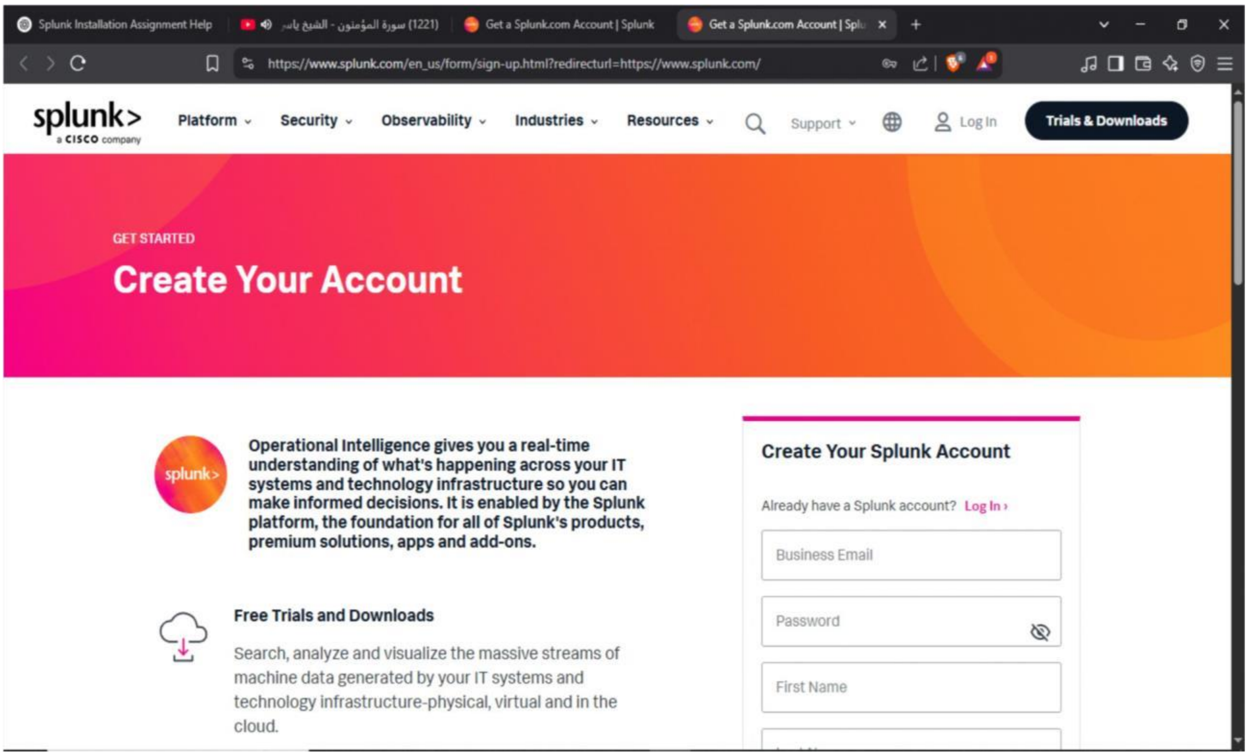
"SETTING UP SPLUNK ENTERPRISE WITH UNIVERSAL FORWARDER ON UBUNTU FOR EFFICIENT LOG COLLECTION AND REAL-TIME MONITORING".

Step 1: Installation of Splunk® Enterprise Server

splunk login/singup link :

https://www.splunk.com/en_us/form/signup.html?redirecturl=https://www.splunk.com/



Splunk Installation Assignment Help
Get a Splunk.com Account | Splunk
Get a Splunk.com Account | Splu
https://www.splunk.com/en_us/form/sign-up.html?redirecturl=https://www.splunk.com/
splunk> a CISCO company
Platform
Security
Observability
Industries
Resources
Support
Log In
Trials & Downloads

GET STARTED

Create Your Account

Operational Intelligence gives you a real-time understanding of what's happening across your IT systems and technology infrastructure so you can make informed decisions. It is enabled by the Splunk platform, the foundation for all of Splunk's products, premium solutions, apps and add-ons.

Free Trials and Downloads

Search, analyze and visualize the massive streams of machine data generated by your IT systems and technology infrastructure-physical, virtual and in the cloud.

Create Your Splunk Account

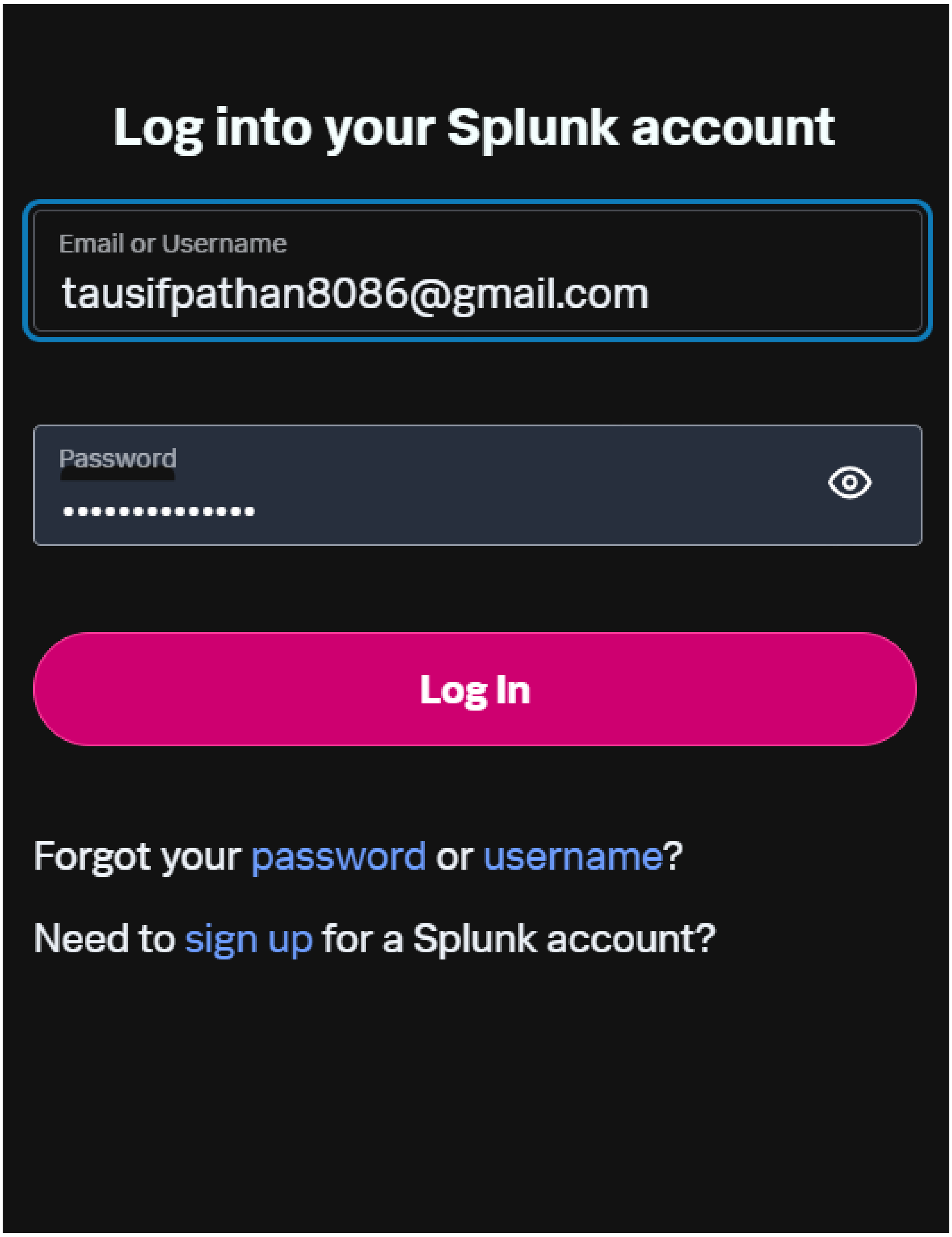
Already have a Splunk account? Log In ›

Business Email

Password

First Name

🔍→Now login in Splunk account



Log into your Splunk account

Email or Username

tausifpathan8086@gmail.com

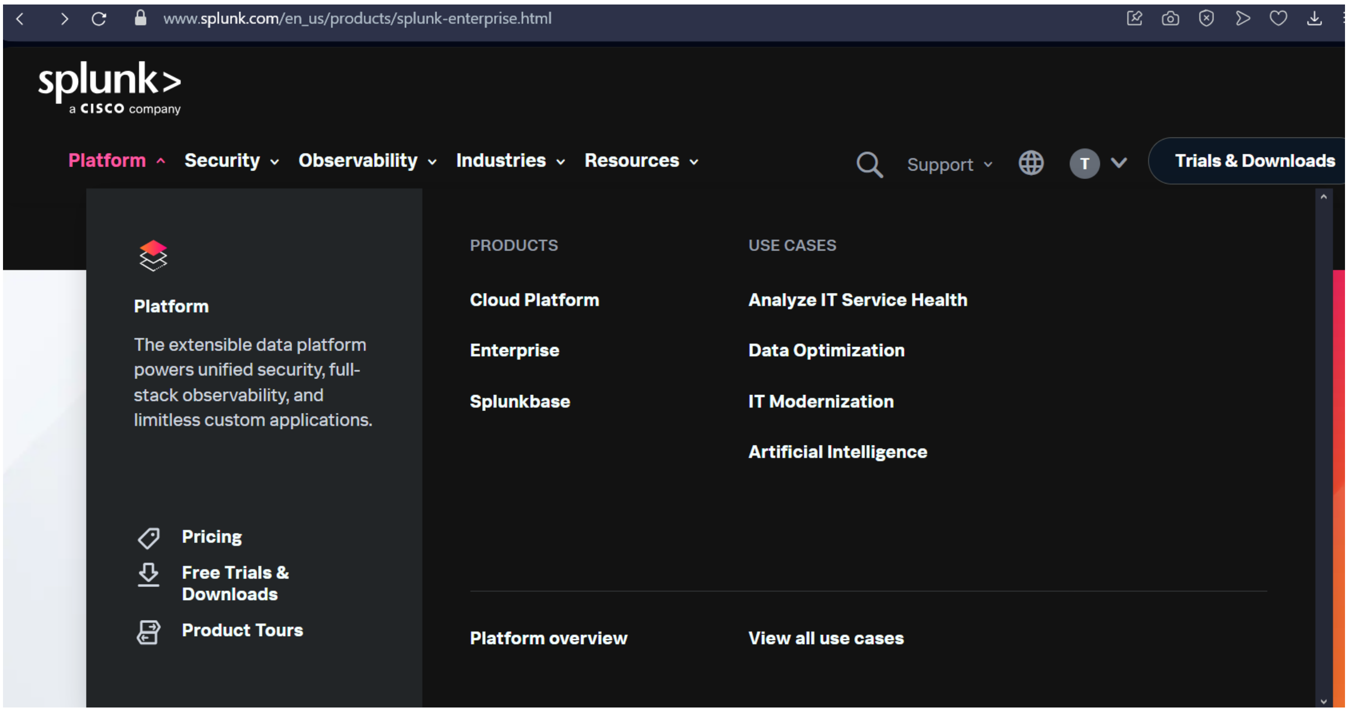
Password

•••••••••••••••

Forgot your password or username?

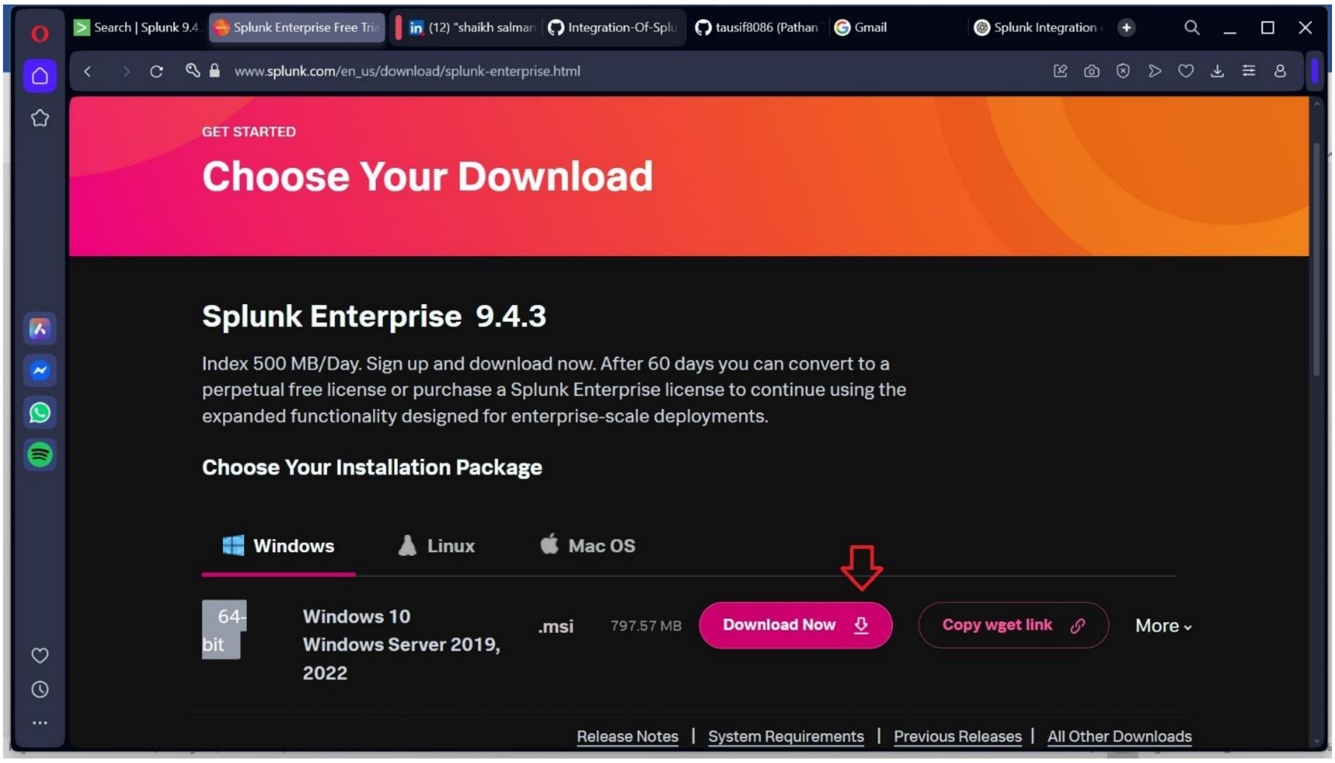
Need to sign up for a Splunk account?

 Now go to platform and click on free trails and downloads



The extensible data platform powers unified security, full-stack observability, and limitless custom applications.

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



Choose Your Download

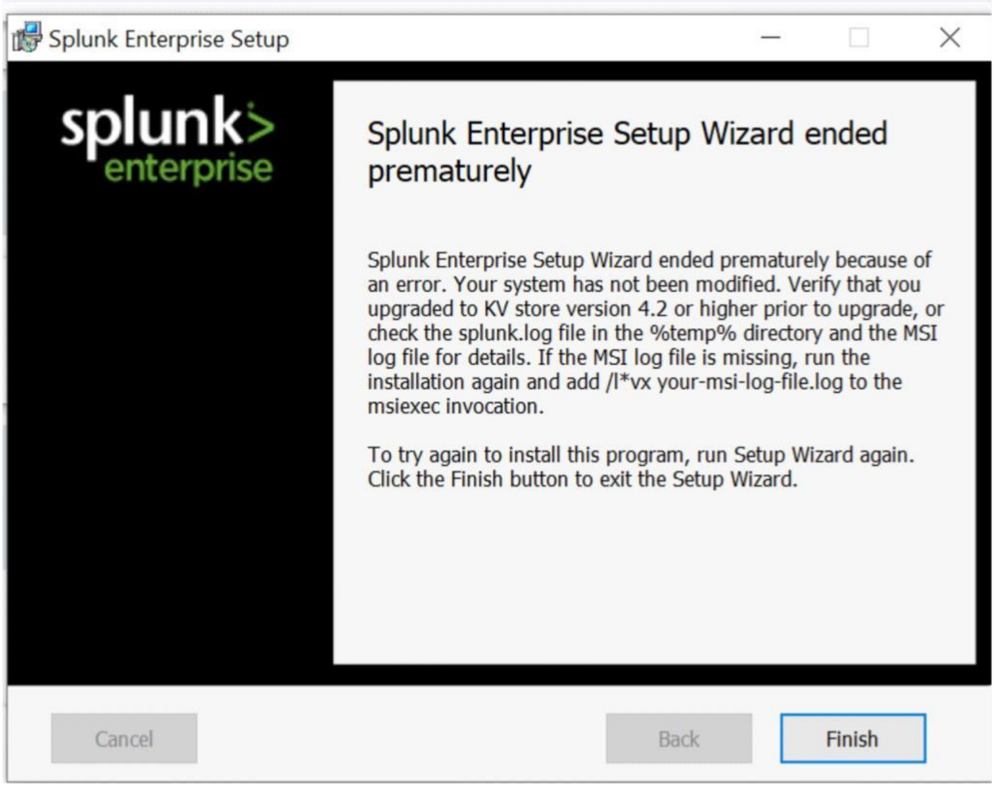
Splunk Enterprise 9.4.3

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 Windows 10 Windows Server 2019, 2022 .msi 797.57 MB

Install download package and create login credential for Splunk server

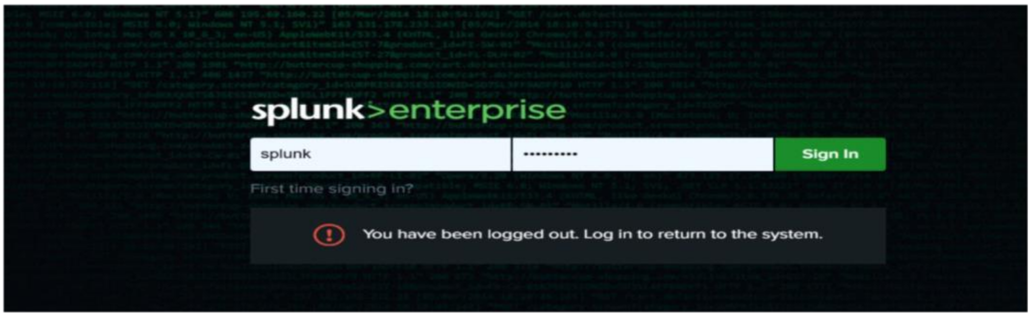


Splunk Enterprise Setup Wizard ended prematurely

Splunk Enterprise Setup Wizard ended prematurely because of an error. Your system has not been modified. Verify that you upgraded to KV store version 4.2 or higher prior to upgrade, or check the splunk.log file in the %temp% directory and the MSI log file for details. If the MSI log file is missing, run the installation again and add /l*vx your-msi-log-file.log to the msiexec invocation.

To try again to install this program, run Setup Wizard again. Click the Finish button to exit the Setup Wizard.

Now login into your Splunk enterprise server

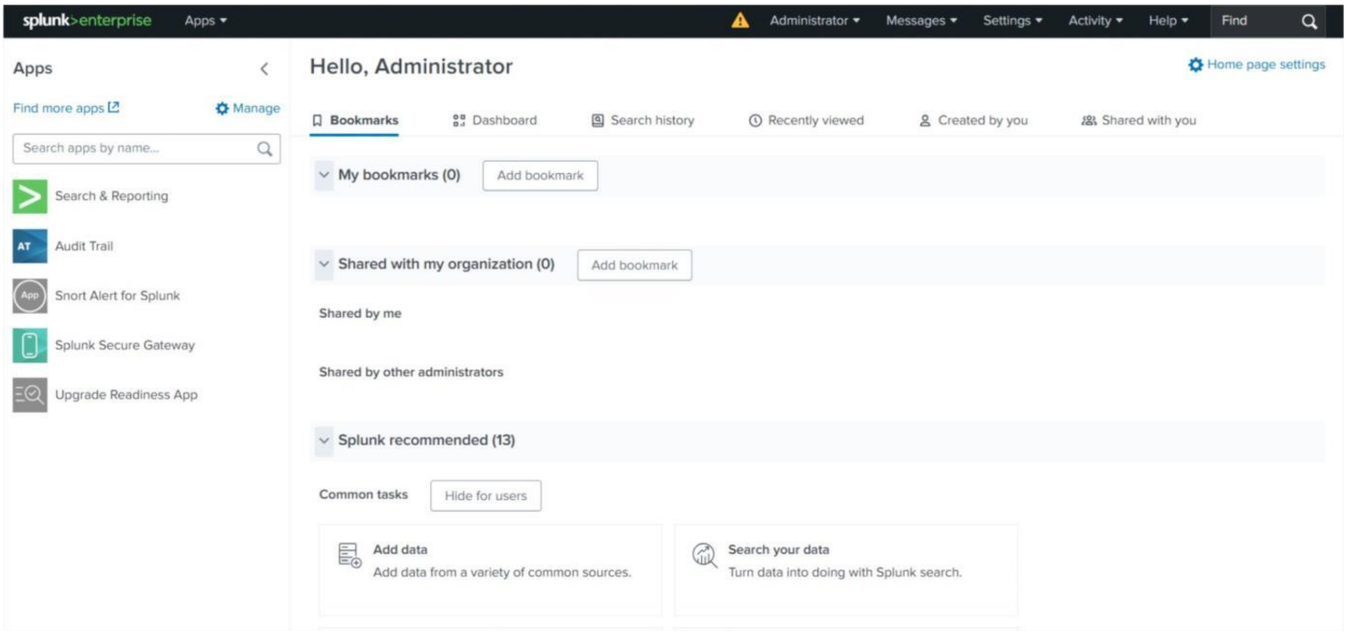


splunk

•••••••••

You have been logged out. Log in to return to the system.

After that Dashboard of Splunk enterprise server appears like this,



Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

Shared by me

Shared by other administrators

Splunk recommended (13)

Common tasks

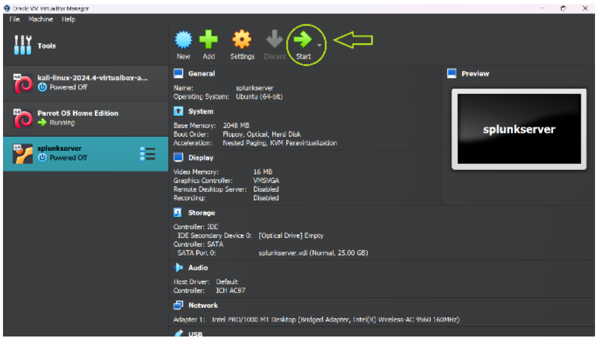
Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

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

o

2Step 2 :- install ubuntu server for forwarding logs to Splunk enterprise Server im using VirtualBox in I have installed ubuntu Server



General
Name: splunkserver
Operating System: Ubuntu (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

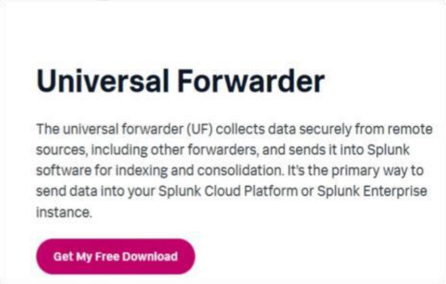
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: splunkserver.vdi (Normal, 25.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Wireless-AC 9560 160MHz)

USB

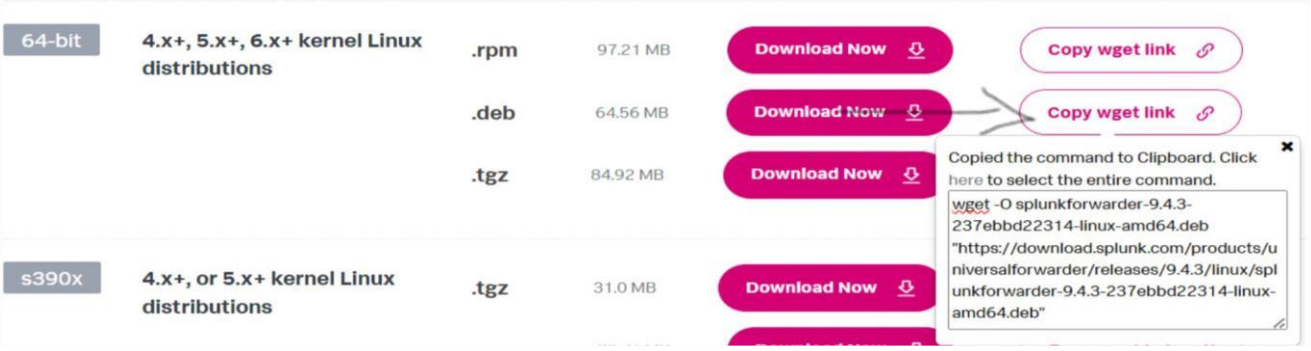
After Successfully installation of ubuntu server get a link of forwarding server based on ubuntu server like Debian package follow same process for login in Splunk https://www.splunk.com/en_us/form/sign-up.html?redirecturl=https://www.splunk.com/ after that go to universal forwarder.



Universal Forwarder

The universal forwarder (UF) collects data securely from remote sources, including other forwarders, and sends it into Splunk software for indexing and consolidation. It's the primary way to send data into your Splunk Cloud Platform or Splunk Enterprise instance.

Chooseinstallationpackage{linux}



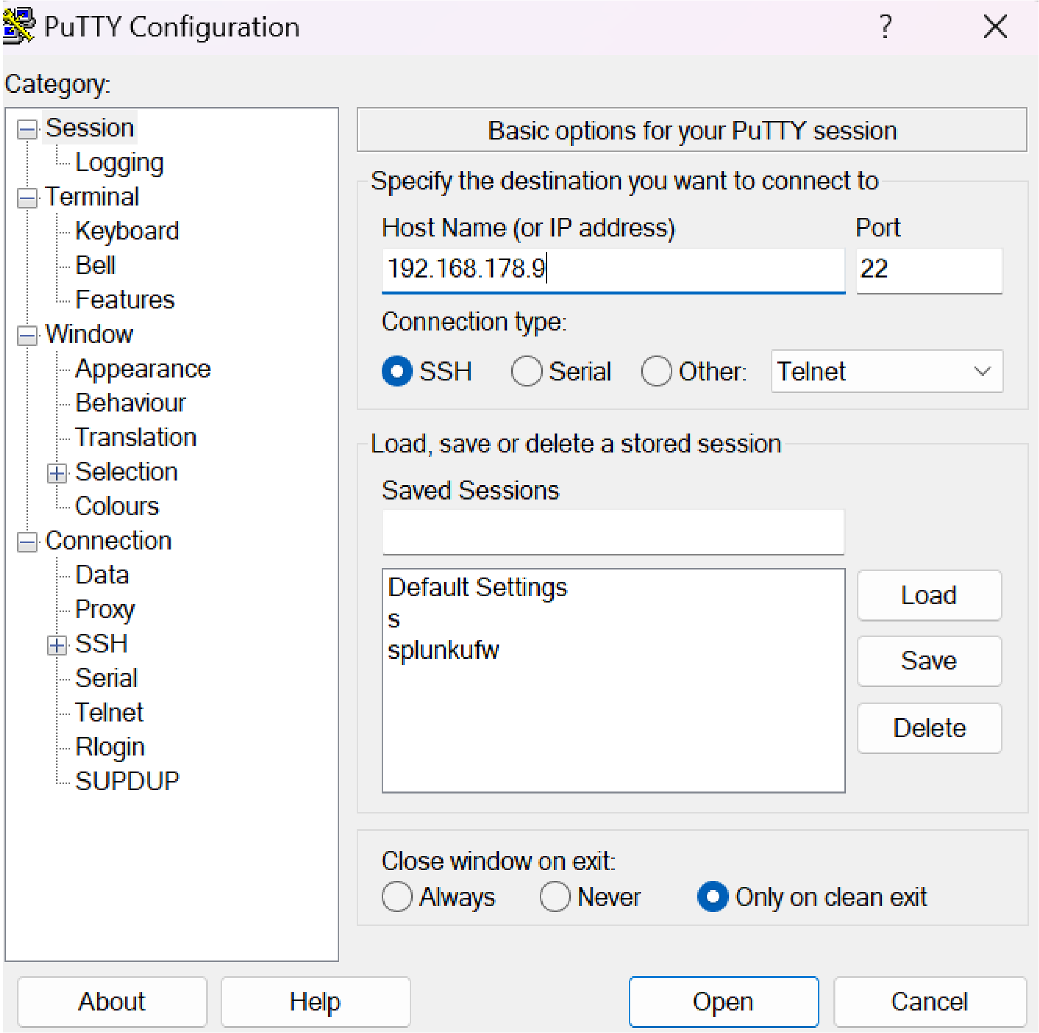
64-bit	4.x+, 5.x+, 6.x+ kernel Linux distributions	.rpm	97.21 MB	Download Now	Copy wget link
		.deb	64.56 MB	Download Now	Copy wget link
		.tgz	84.92 MB	Download Now	
s390x	4.x+, or 5.x+ kernel Linux distributions	.tgz	31.0 MB	Download Now	

Copied the command to Clipboard. Click here to select the entire 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 serverand Putti using ssh.



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.178.9

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

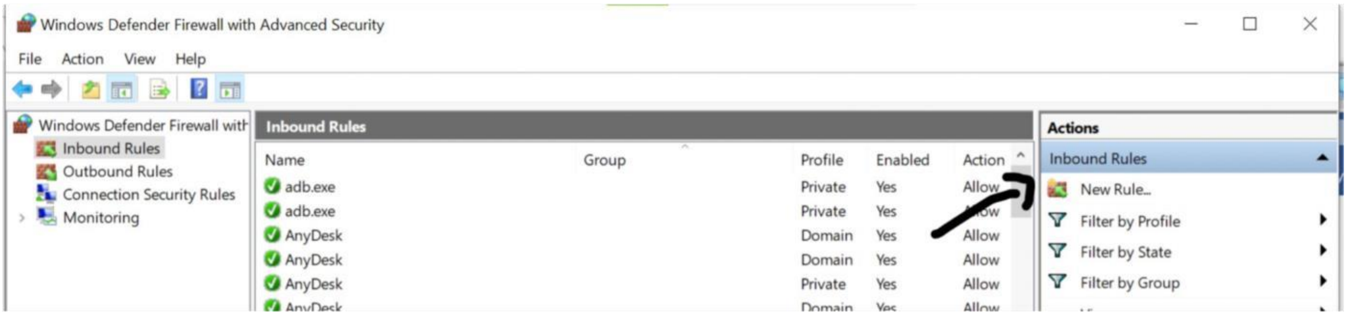
Load, save or delete a stored session

Saved Sessions

Default Settings
s
splunkufw

Close window on exit: ○ Always ○ Never ● Only on clean exit

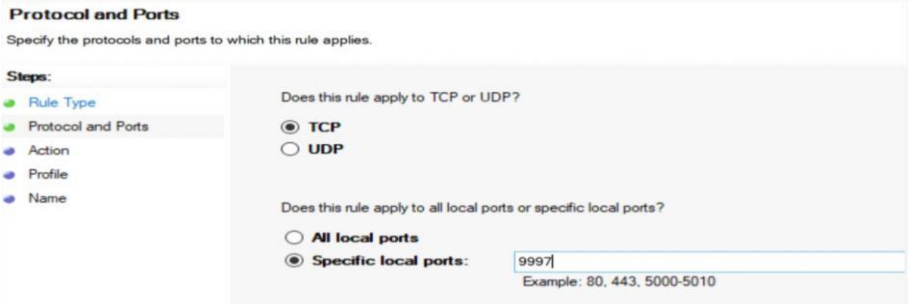
After established a connection successfully create a inbound rule in windows go to firewall & networks select Advance setting and create it as shown in screenshots below.



Name	Group	Profile	Enabled	Action
adb.exe		Private	Yes	Allow
adb.exe		Private	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Private	Yes	Allow
AnyDesk		Domain	Yes	Allow

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.

Does this rule apply to TCP or UDP?

● TCP

○ UDP

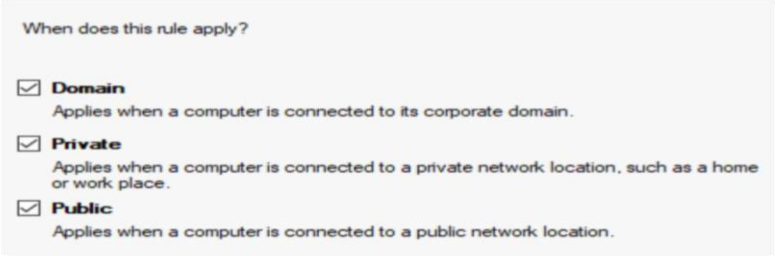
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 9997

Example: 80, 443, 5000-5010

allow the connection and click on next

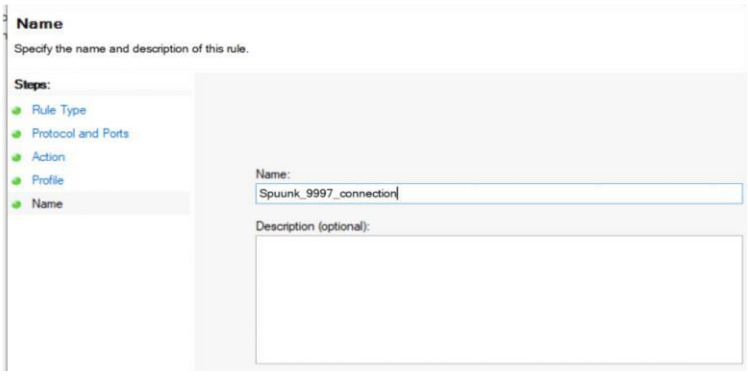

When does this rule apply?

☑ **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

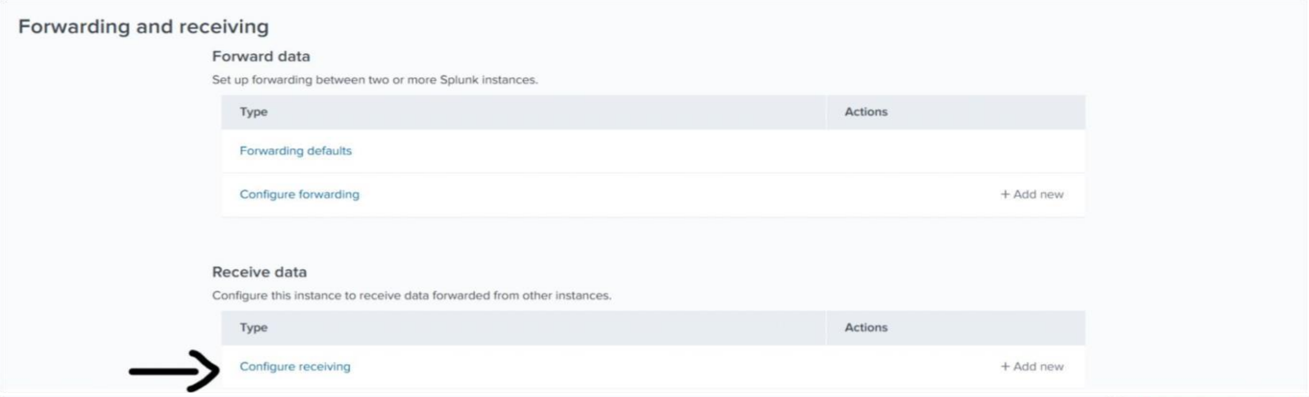

Name

Specify the name and description of this rule.

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

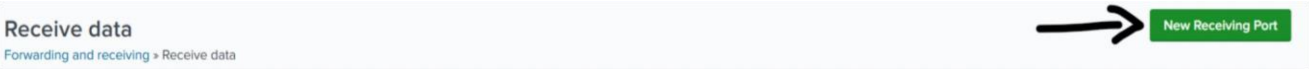
Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

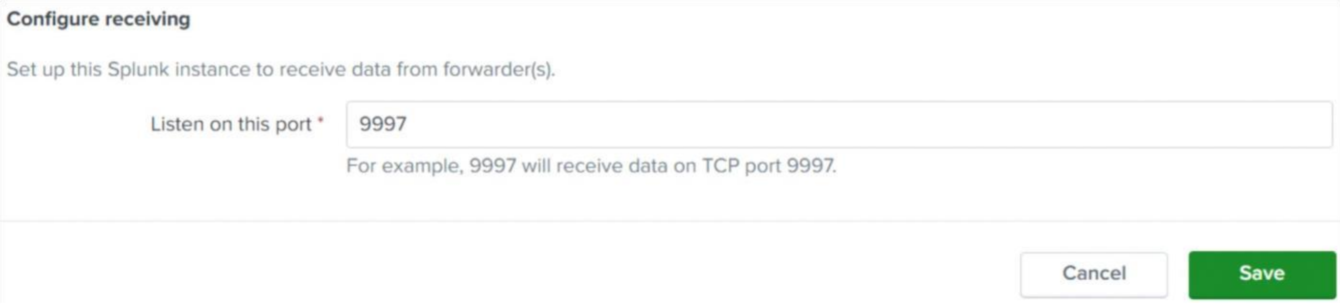
Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new



Receive data

Forwarding and receiving » Receive data



Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port * 9997

For example, 9997 will receive data on TCP port 9997.

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)

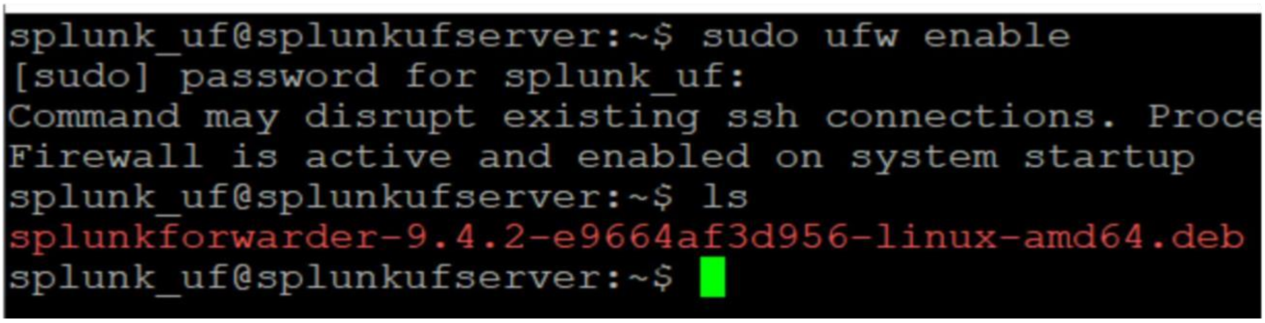
#sudo ufw allow 9997/tcp (for receiving port)

# 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

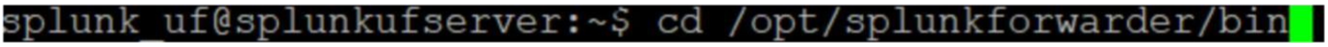
#sudo dpkg -I splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb (package name)

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



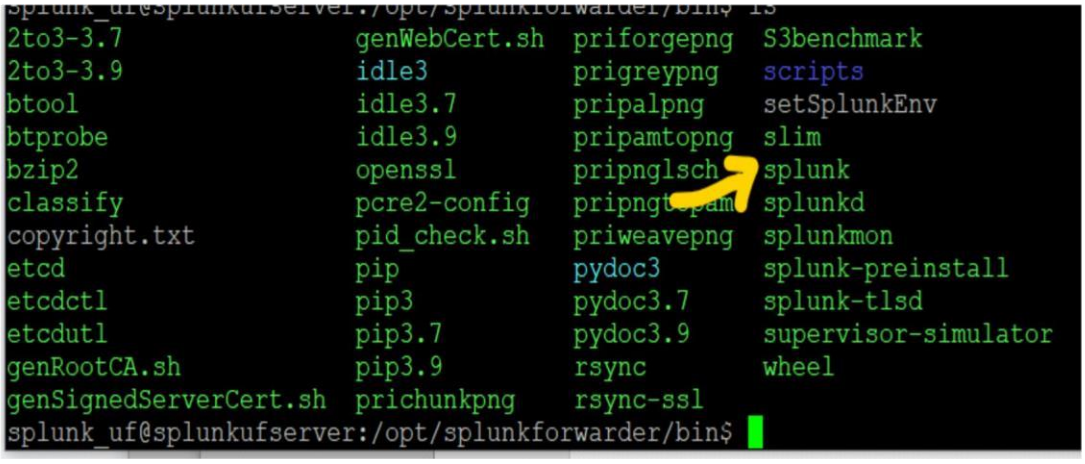
```
splunk_uf@splunkufserver:~$ sudo ufw enable
[sudo] password for splunk_uf:
Command may disrupt existing ssh connections. Proce
Firewall is active and enabled on system startup
splunk_uf@splunkufserver:~$ ls
splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb
splunk_uf@splunkufserver:~$ 
```

For run a Splunk forwarder follow this path



```
splunk_uf@splunkufserver:~$ cd /opt/splunkforwarder/bin
```

# ls (for list of file and directories)

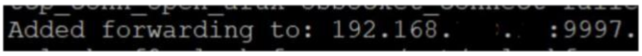


```
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ ls
2to3-3.7                 genWebCert.sh  priforgepng    S3benchmark
2to3-3.9                 idle3          prigreypng     scripts
btool                    idle3.7        pripalpng      setSplunkEnv
btprobe                  idle3.9        pripamtopng    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 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.



```
Added forwarding to: 192.168.[redacted]:9997.
```

(Splunk enterprise server added successfully)

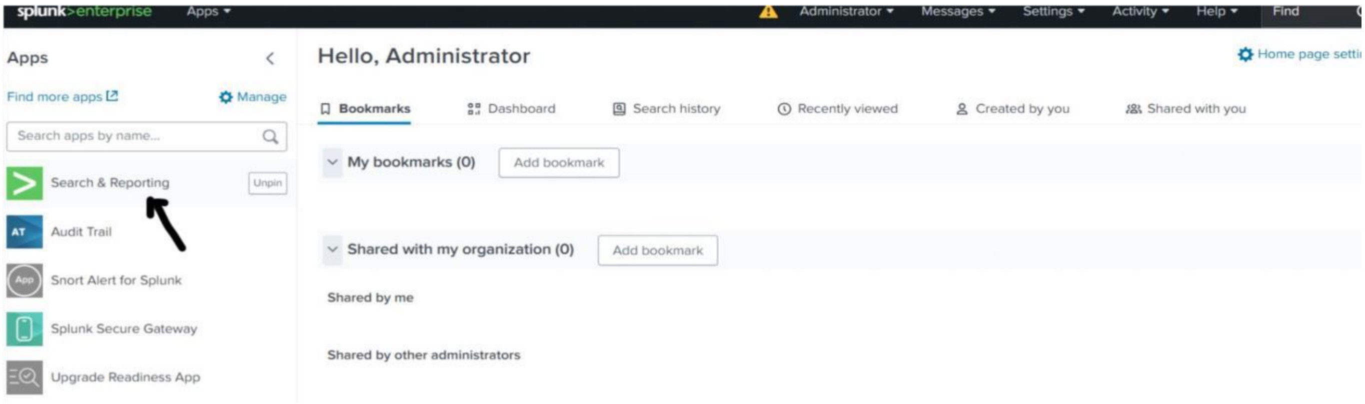
Restart Splunk

#sudo ./splunk restart

Step 2 after added server

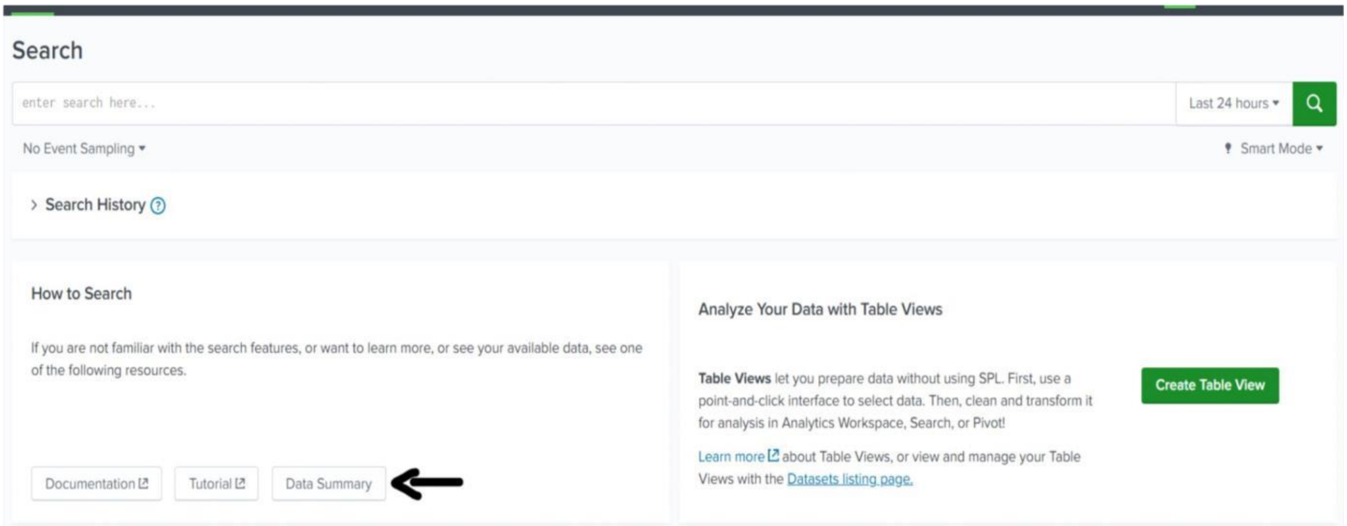
# sudo ./splunk add monitor /var/log

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



Go to Splunk enterprise server and select search and report.

Click on data Summary



How to Search

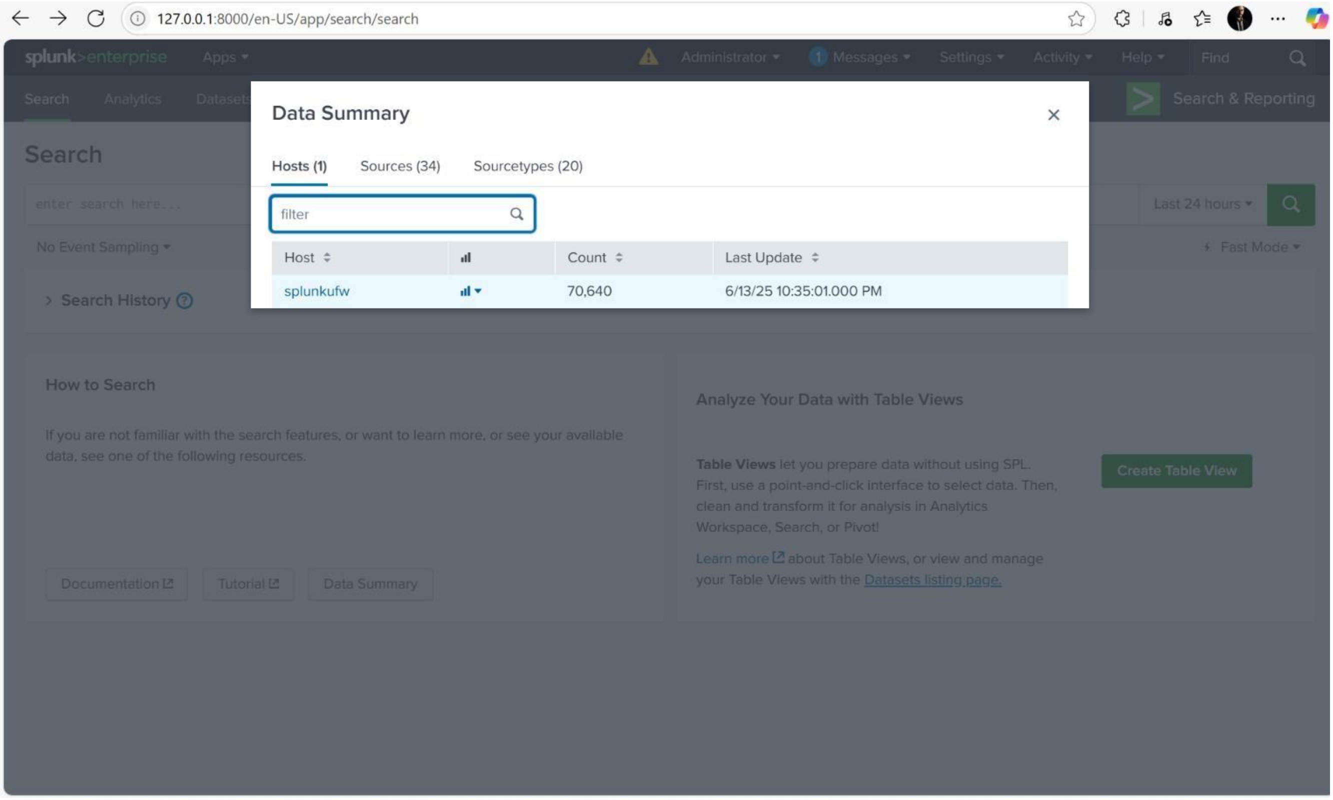
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views

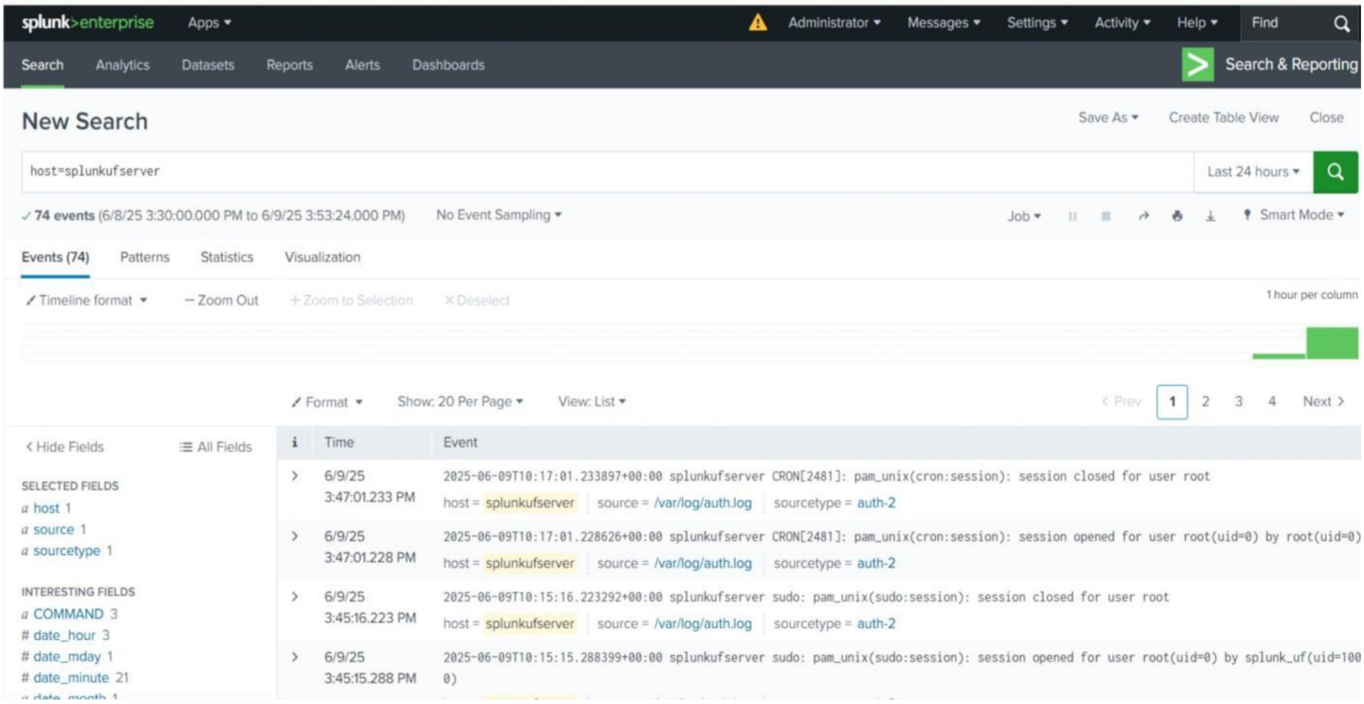
Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

🛡Click on host ,



Host		Count	Last Update
splunkufw		70,640	6/13/25 10:35:01.000 PM



```
host=splunkufserver
```

✓ 74 events (6/8/25 3:30:00.000 PM to 6/9/25 3:53:24.000 PM)

i	Time	Event

>	6/9/25 3:47:01.233 PM	`2025-06-09T10:17:01.233897+00:00 splunkufserver CRON[2481]: pam_unix(cron:session): session closed for user root`
		host = splunkufserver · source = /var/log/auth.log · sourcetype = auth-2

>	6/9/25 3:47:01.228 PM	`2025-06-09T10:17:01.228626+00:00 splunkufserver CRON[2481]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)`
		host = splunkufserver · source = /var/log/auth.log · sourcetype = auth-2

>	6/9/25 3:45:16.223 PM	`2025-06-09T10:15:16.223292+00:00 splunkufserver sudo: pam_unix(sudo:session): session closed for user root`
		host = splunkufserver · source = /var/log/auth.log · sourcetype = auth-2

>	6/9/25 3:45:15.288 PM	`2025-06-09T10:15:15.288399+00:00 splunkufserver sudo: pam_unix(sudo:session): session opened for user root(uid=0) by splunk_uf(uid=1000)`

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

✍ Overview:

This configuration showcases the successful implementation of **Splunk® Enterprise** alongside the **Universal Forwarder** on an **Ubuntu** system, facilitating streamlined log collection and centralized monitoring.

It lays the groundwork for:

🔐 **Security Monitoring**
□ **System Compliance and Auditing**
📈 **Live Log Tracking and Analysis**

This setup enhances organizational visibility into system operations and strengthens the ability to detect and respond to security events effectively.