🔐 Built My Own Splunk SIEM Homelab from Scratch

Recently I finished setting up a **SIEM homelab using Splunk on Ubuntu** to practice log analysis, detection use cases, and blue-team skills.

Here’s how I built it step by step

Objective

- Install and configure **Splunk Enterprise (free license)** on an **Ubuntu VM**
- Ingest sample log data into Splunk
- Run basic searches, build visualizations, and explore security use cases

---

1. Lab Environment Setup

Tools I used:

- Hypervisor: `VMware`
- OS: `Ubuntu Desktop` (22.04)
- SIEM: `Splunk Enterprise (Free)`

VM Specs (example):

- CPU: 2 vCPUs
- RAM: 4–8 GB
- Disk: 40–60 GB

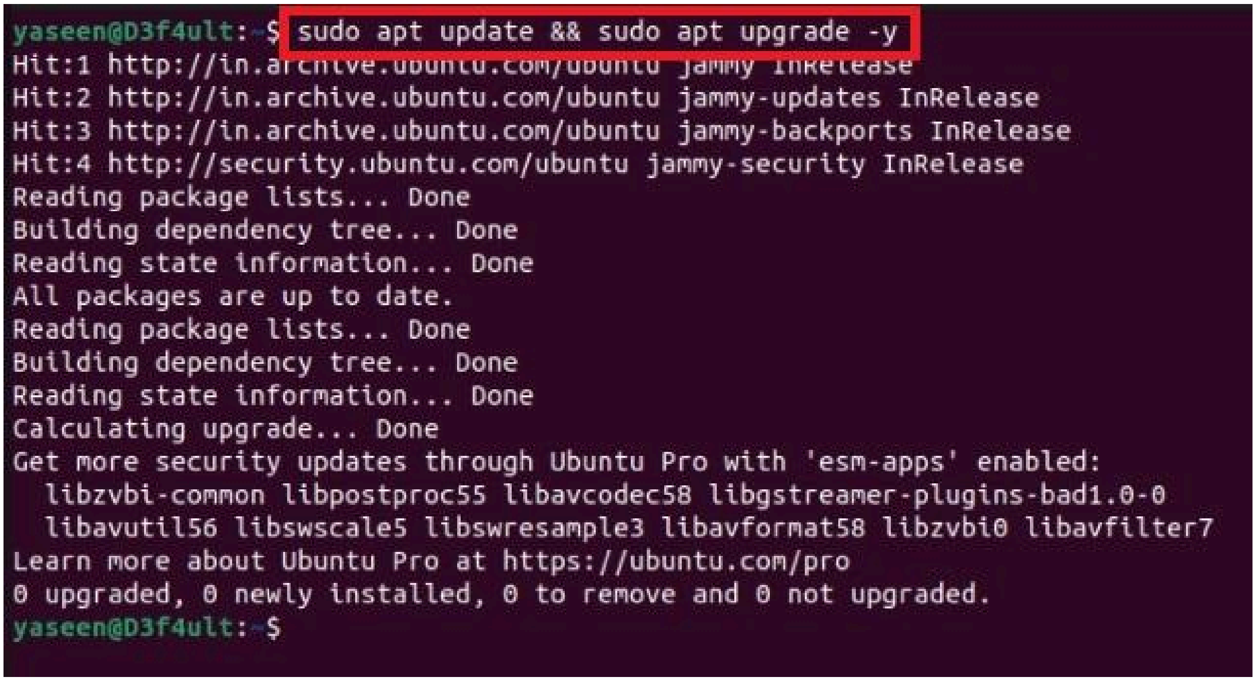
After creating the VM, I mounted the Ubuntu ISO and installed the OS with a normal guided installation.

---

2. Update & Prepare Ubuntu

Once Ubuntu was installed, I logged in and updated the system:

```
sudo apt update && sudo apt upgrade -y
```



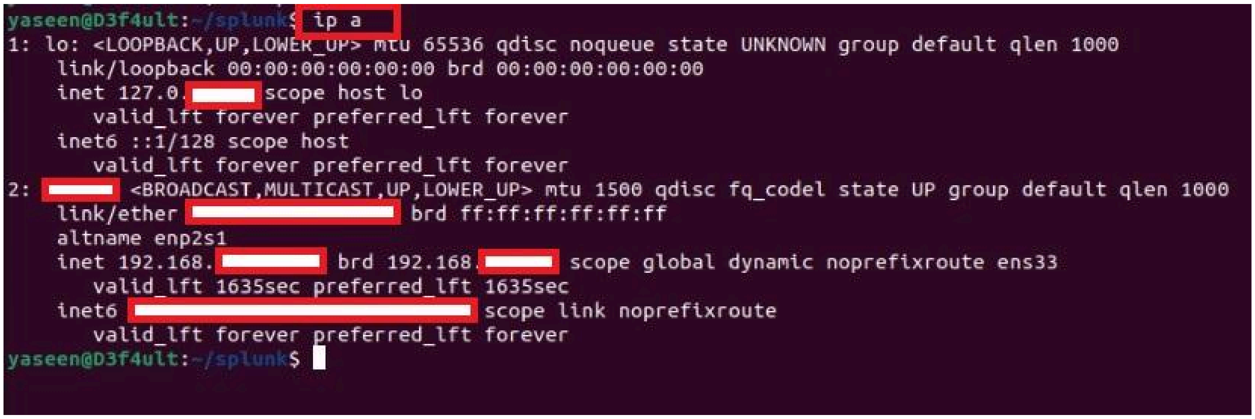
```
yaseen@D3f4ult:~$ sudo apt update && sudo apt upgrade -y
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
  libzvbi-common libpostproc55 libavcodec58 libgstreamer-plugins-bad1.0-0
  libavutil56 libswscale5 libswresample3 libavformat58 libzvbi0 libavfilter7
Learn more about Ubuntu Pro at https://ubuntu.com/pro
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
yaseen@D3f4ult:~$
```

(Optional but good practice) Install some basic tools:

```
sudo apt install -y wget curl vim net-tools
```

To check the IP of my VM (needed later to access Splunk Web):

```
ip a
```



```
yaseen@D3f4ult:~/splunk$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.[redacted] scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: [redacted] <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.[redacted] brd 192.168.[redacted] scope global dynamic noprefixroute ens33
       valid_lft 1635sec preferred_lft 1635sec
    inet6 [redacted] scope link noprefixroute
       valid_lft forever preferred_lft forever
yaseen@D3f4ult:~/splunk$
```

So first we will create a directory and named splunk:

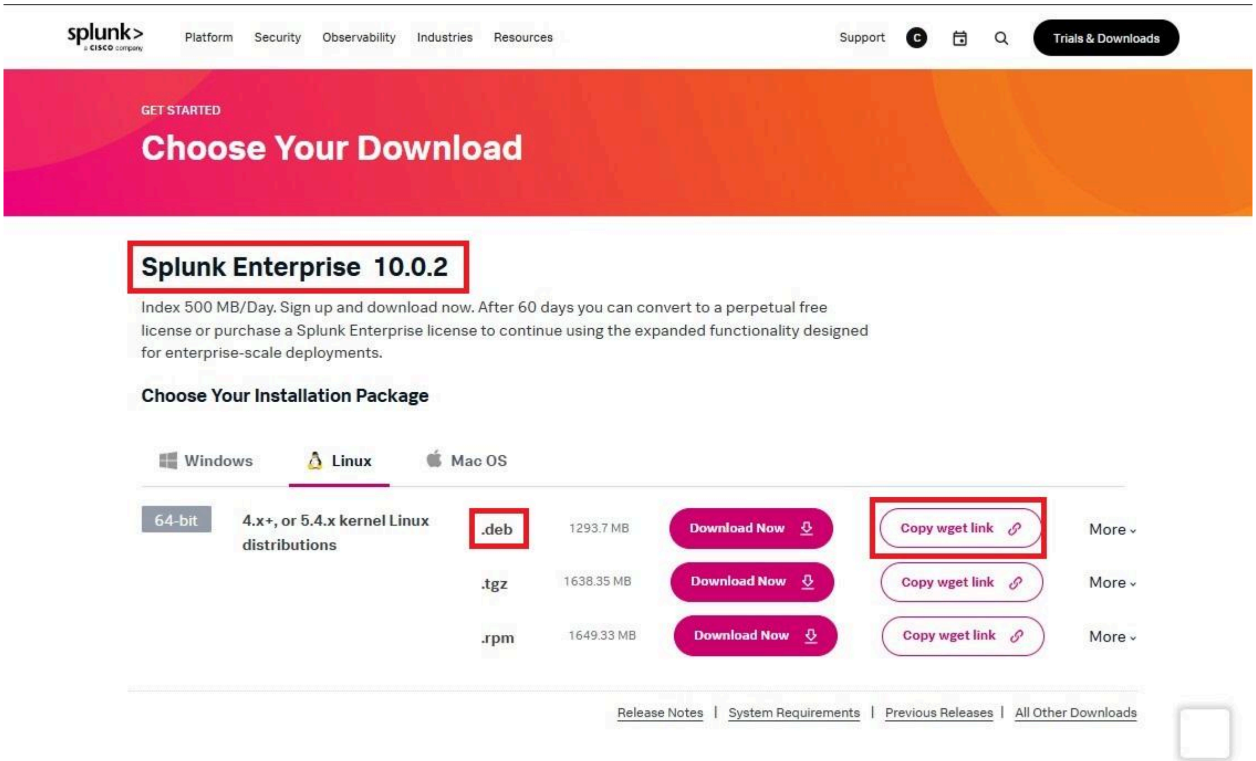
```
mkdir splunk
```

---

3. Download & Install Splunk

I then downloaded the **Splunk .deb** package for Linux (using `wget` with the download link from my Splunk account).

```
cd /splunk

wget -O splunk-10.0.2-e2d18b4767e9-linux-amd64.deb
"https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.deb"
```



GET STARTED

Choose Your Download

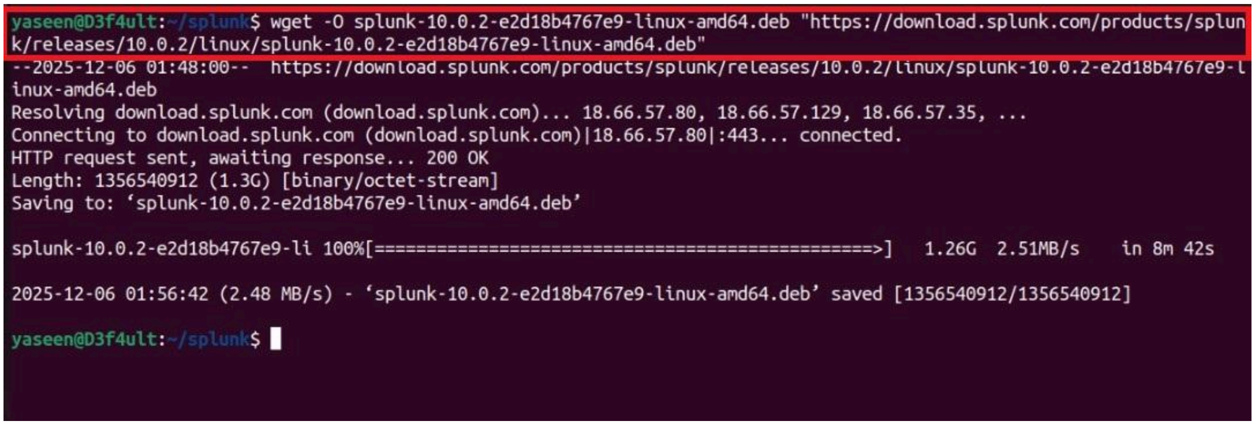
Splunk Enterprise 10.0.2

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	4.x+, or 5.4.x kernel Linux distributions	.deb	1293.7 MB	Download Now	Copy wget link	More
		.tgz	1638.35 MB	Download Now	Copy wget link	More
		.rpm	1649.33 MB	Download Now	Copy wget link	More

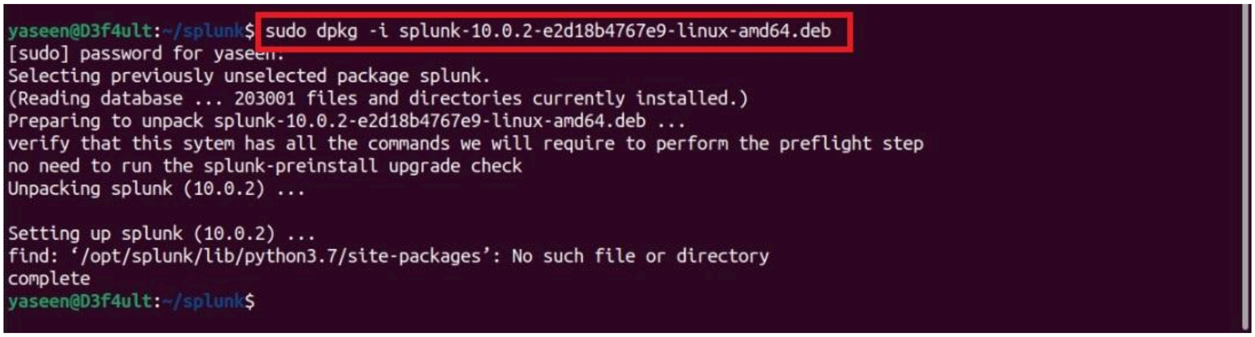
Release Notes | System Requirements | Previous Releases | All Other Downloads



```
yaseen@D3f4ult:~/splunk$ wget -O splunk-10.0.2-e2d18b4767e9-linux-amd64.deb "https://download.splunk.com/products/splun
k/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.deb"
--2025-12-06 01:48:00--  https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-l
inux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 18.66.57.80, 18.66.57.129, 18.66.57.35, ...
Connecting to download.splunk.com (download.splunk.com)|18.66.57.80|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1356540912 (1.3G) [binary/octet-stream]
Saving to: ‘splunk-10.0.2-e2d18b4767e9-linux-amd64.deb’

splunk-10.0.2-e2d18b4767e9-li 100%[===============================================>]   1.26G  2.51MB/s    in 8m 42s

2025-12-06 01:56:42 (2.48 MB/s) - ‘splunk-10.0.2-e2d18b4767e9-linux-amd64.deb’ saved [1356540912/1356540912]

yaseen@D3f4ult:~/splunk$ 
```

Install the package:

```
sudo dpkg -i splunk-10.0.2-e2d18b4767e9-linux-amd64.deb
```



```
yaseen@D3f4ult:~/splunk$ sudo dpkg -i splunk-10.0.2-e2d18b4767e9-linux-amd64.deb
[sudo] password for yaseen:
Selecting previously unselected package splunk.
(Reading database ... 203001 files and directories currently installed.)
Preparing to unpack splunk-10.0.2-e2d18b4767e9-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunk (10.0.2) ...

Setting up splunk (10.0.2) ...
find: '/opt/splunk/lib/python3.7/site-packages': No such file or directory
complete
yaseen@D3f4ult:~/splunk$
```

Splunk is installed by default in:

```
/opt/splunk
```

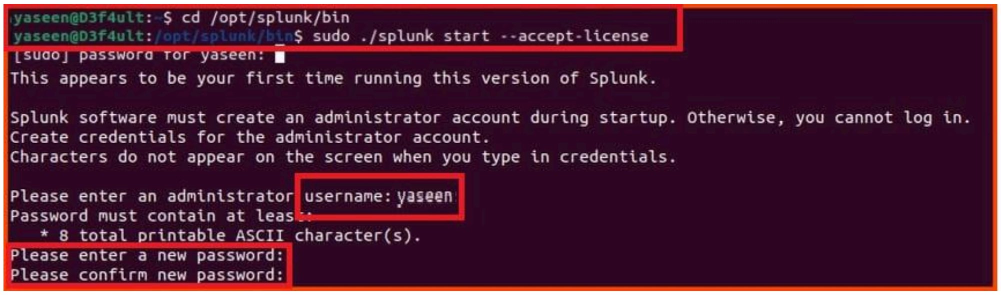
4. Start Splunk & Accept the License

Go to the Splunk directory:

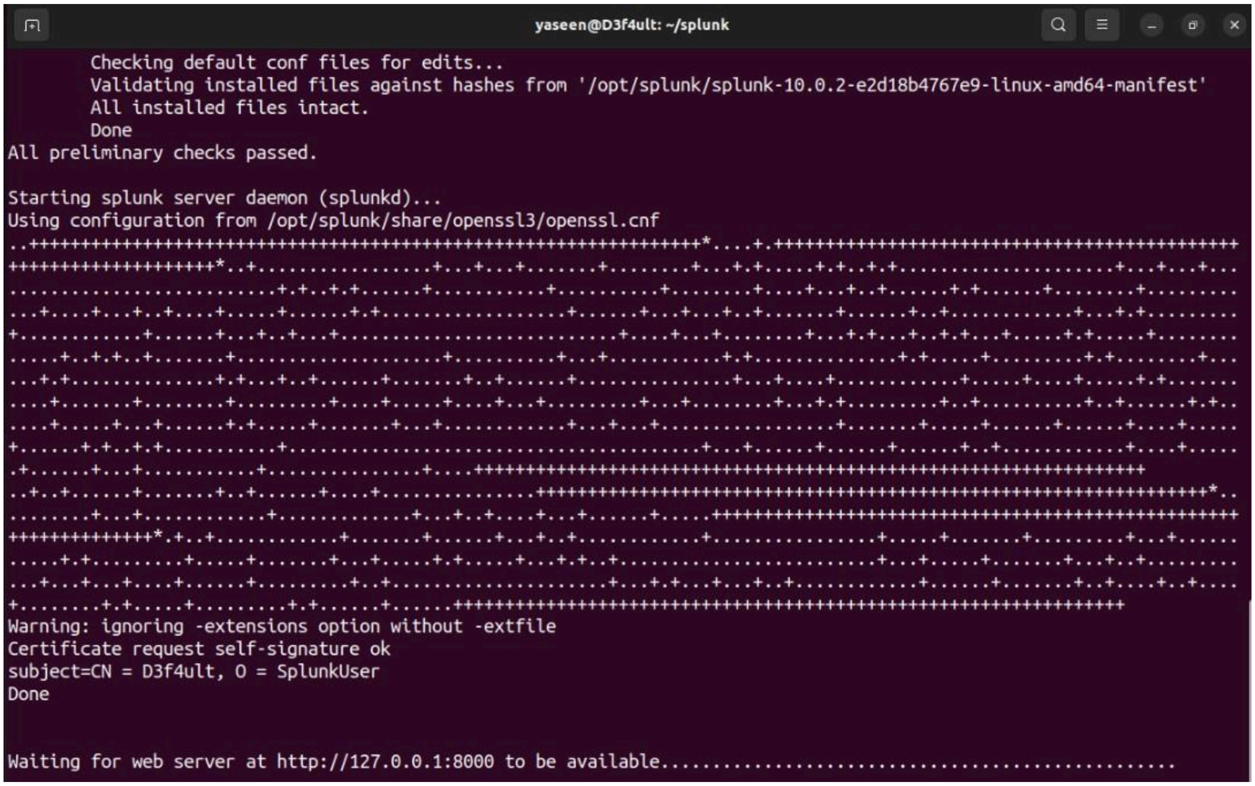
```
cd /opt/splunk/bin
```

Start Splunk for the first time and accept the license:

```
sudo ./splunk start --accept-license
```



```
yaseen@D3f4ult:~$ cd /opt/splunk/bin
yaseen@D3f4ult:/opt/splunk/bin$ sudo ./splunk start --accept-license
[sudo] password for yaseen:
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: yaseen
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

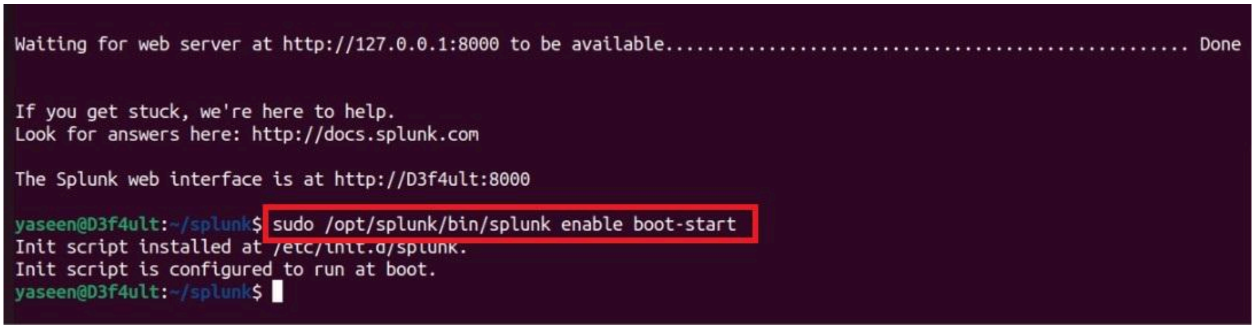


```
yaseen@D3f4ult: ~/splunk
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-10.0.2-e2d18b4767e9-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Using configuration from /opt/splunk/share/openssl3/openssl.cnf
..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....+.+++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++*..+.................+...+...+.......+.......+...+.+.....+.+..+.+........................+...+...+...
.........................+.+..+.+......+...........+..........+........+....+...+..+......+.+......+........+.........
...+....+...+..+....+.....+......+.+.................+......+...+...+.+.......+......+..+.............+...+.+.........
+............+......+...+..+...+..........................+....+...+........+...+.+...+.+.+...+.....+.+.....+.........
.....+..+.+..+.......+....................+..........+...+...........+.+..............+.+.....+.........+.+........+...
...+.+..............+.+...+..+.......+.......+..+......+...............+...+....+..............+.....+....+.....+.+.......
....+........+........+.........+.....+.....+....+...+..........+...+.........+...+.+..........+..+...........+..+.......+.+..
....+.....+...+......+.+.....+.......+...+............+...+...+...................+.......+.....+.......+......+....+.....
+......+.+..+.+..........+........................................+...+......+.....+......+..+............+....+.....
.+......+...+...........+.................+....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+..+......+.......+..+......+....+...............+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..
........+...+...........+.............+...+..+...+.....+.....++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++*.+..+...........+.........+......+...+..+...........+................+.....+.......+.........+...+.......
.....+.+.........+.....+.......+...+.....+.+.....+...+.+..+.........................+...+.....+......+...+..+.........
...+...+...+....+......+.........+..+.....................+...+..+...+...+..+............+......+.......+..+....+..+.....
+........+.+.....+.........+.+......+......+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Warning: ignoring -extensions option without -extfile
Certificate request self-signature ok
subject=CN = D3f4ult, O = SplunkUser
Done


Waiting for web server at http://127.0.0.1:8000 to be available.............................................
```

During the first start, Splunk asks to set an **admin username and password**.
I created a strong local admin account and noted it down.

Optional: enable Splunk to start on boot:

```
sudo /opt/splunk/bin/splunk enable boot-start
```



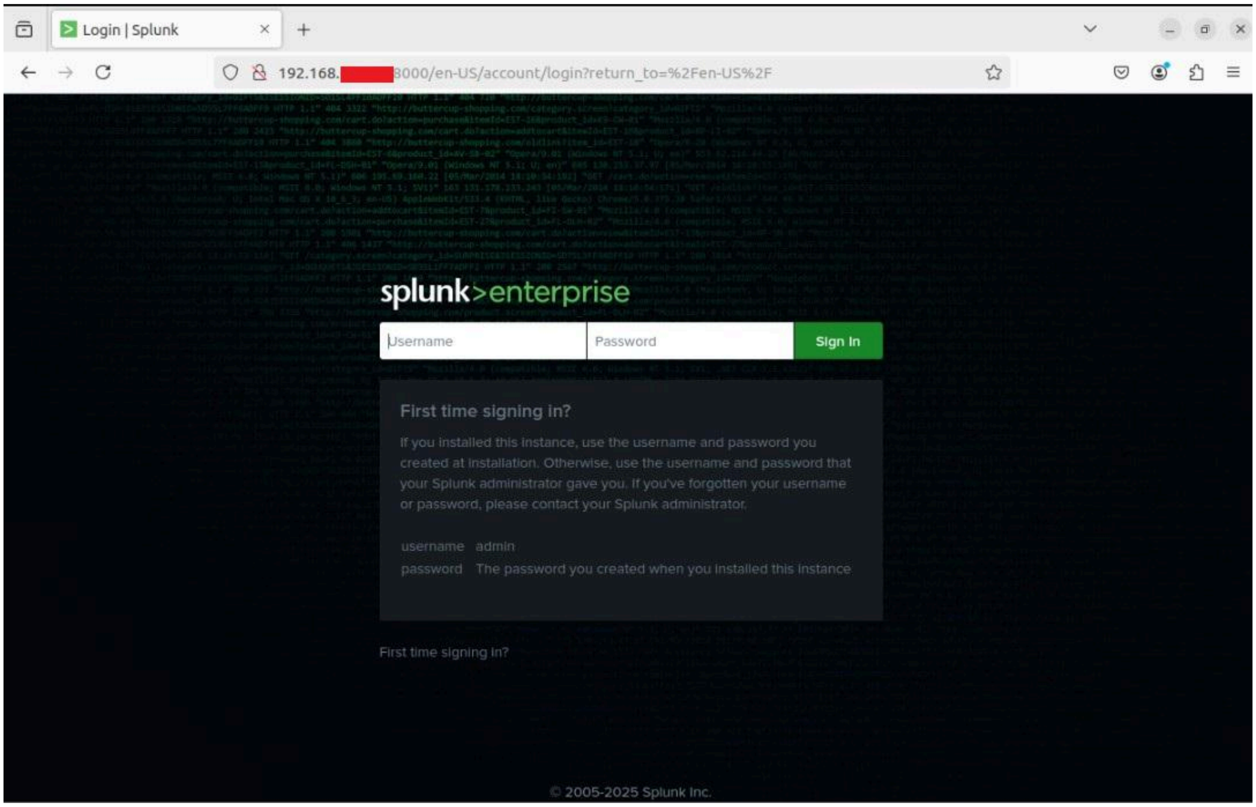
```
Waiting for web server at http://127.0.0.1:8000 to be available.............................................. Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://D3f4ult:8000

yaseen@D3f4ult:~/splunk$ sudo /opt/splunk/bin/splunk enable boot-start
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
yaseen@D3f4ult:~/splunk$ 
```

5. Access Splunk Web Interface

By default, Splunk Web runs on port **8000**.

From my host machine, I opened a browser and went to:

```
http://<Ubuntu_VM_IP>:8000
```



192.168.[redacted]8000/en-US/account/login?return_to=%2Fen-US%2F

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

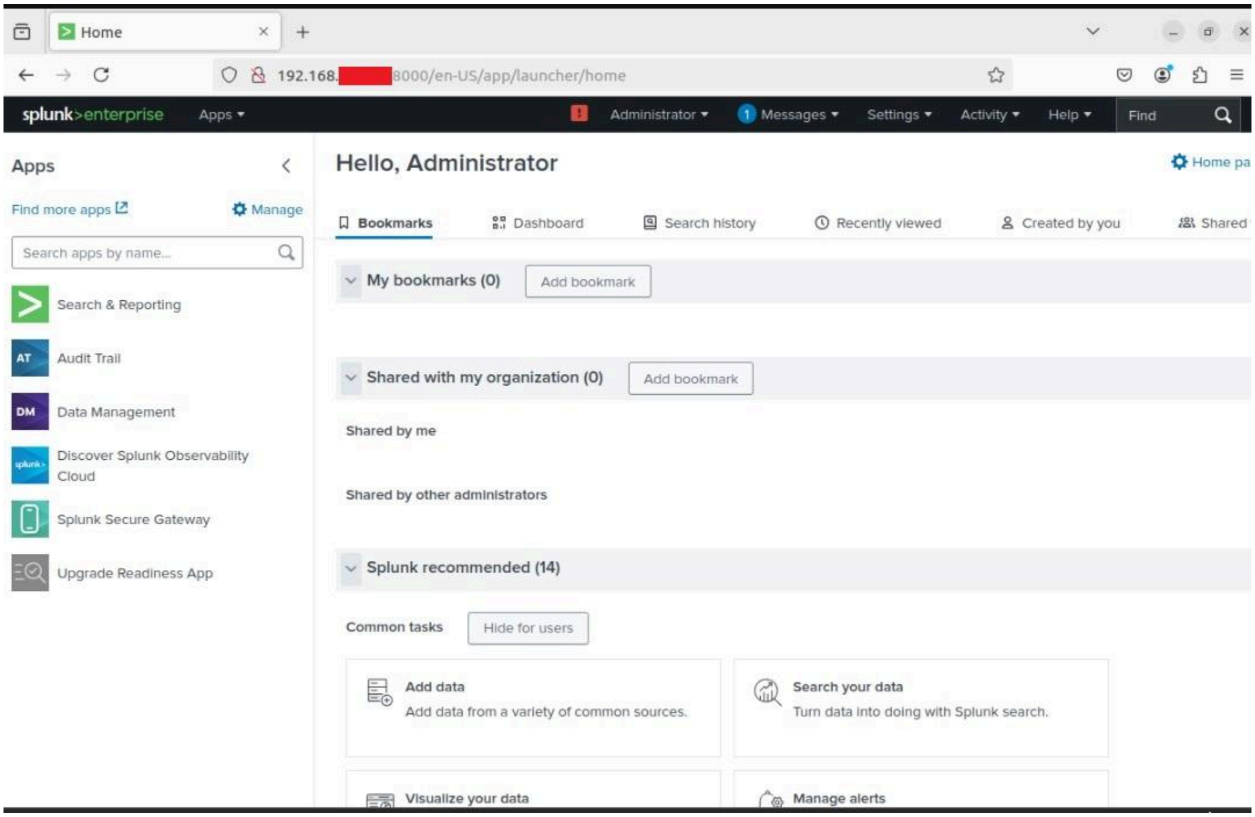
First time signing in?

© 2005-2025 Splunk Inc.

Example:

```
http://192.168.1.60:8000
```

Then I logged in with the `admin` credentials created earlier.



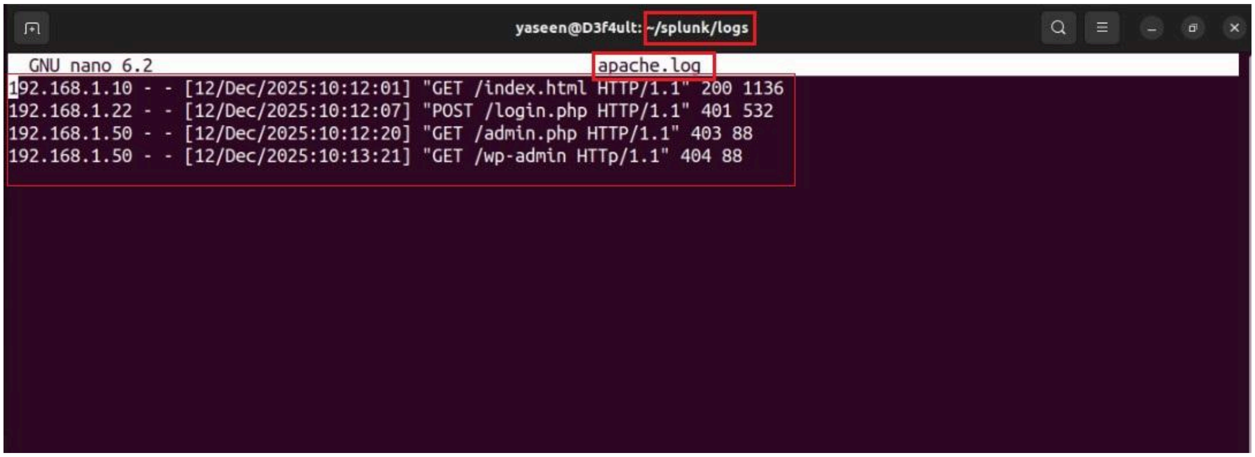
192.168.[redacted]8000/en-US/app/launcher/home

Hello, Administrator

---

6. Add Sample Logs / Data Sources

Next, I ingested data into Splunk that I've created using nano named the files with apache.log to start playing with searches and dashboards.



```
  GNU nano 6.2                            apache.log
192.168.1.10 - - [12/Dec/2025:10:12:01] "GET /index.html HTTP/1.1" 200 1136
192.168.1.22 - - [12/Dec/2025:10:12:07] "POST /login.php HTTP/1.1" 401 532
192.168.1.50 - - [12/Dec/2025:10:12:20] "GET /admin.php HTTP/1.1" 403 88
192.168.1.50 - - [12/Dec/2025:10:13:21] "GET /wp-admin HTTp/1.1" 404 88
```

From **Splunk Web**:

1. Clicked **Settings ➜ Add Data**

2. Selected **Upload** (for local log files like web server logs / security logs)

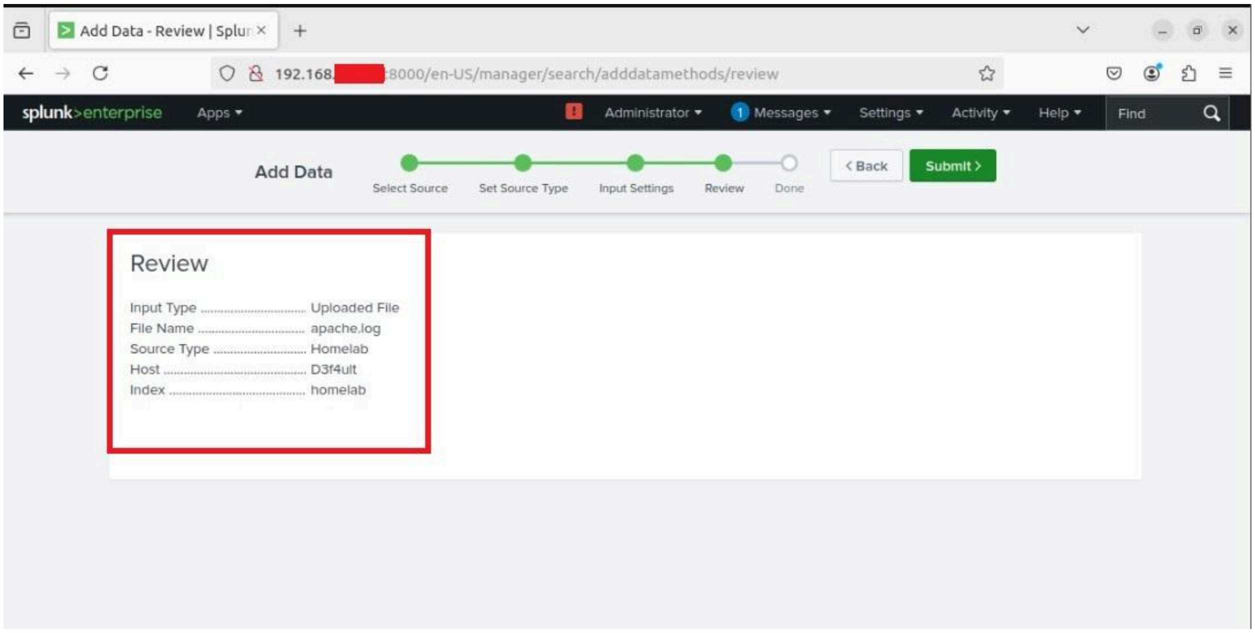
3. Choose my log file(s) (for example: Apache/Nginx access logs, Windows event exports, etc.)

4. Chose:

   ○ **Source type** (e.g., `access_combined`, `iis`, or left it to auto-detect)

   ○ **Index**: created an index `homelab`

5. Clicked **Review ➜ Submit**



Review

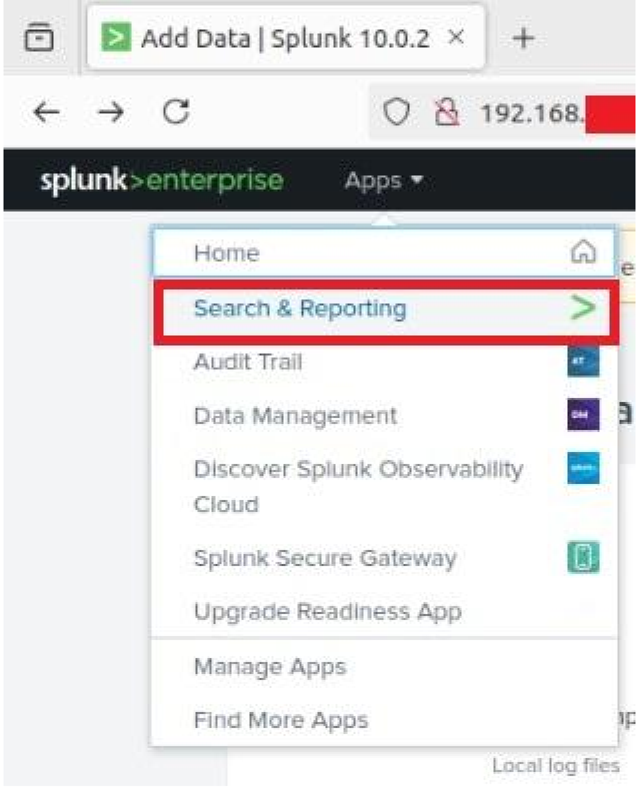
Input Type .... Uploaded File
File Name .... apache.log
Source Type .... Homelab
Host D3f4ult
Index .... homelab

After this, Splunk started indexing the uploaded logs.

---

7. Verify Data Ingestion with Basic Searches

I headed to **Search & Reporting** app and ran some basic searches to confirm that data was coming in:



All events:

```
index=* | head 20
```

Events by index:

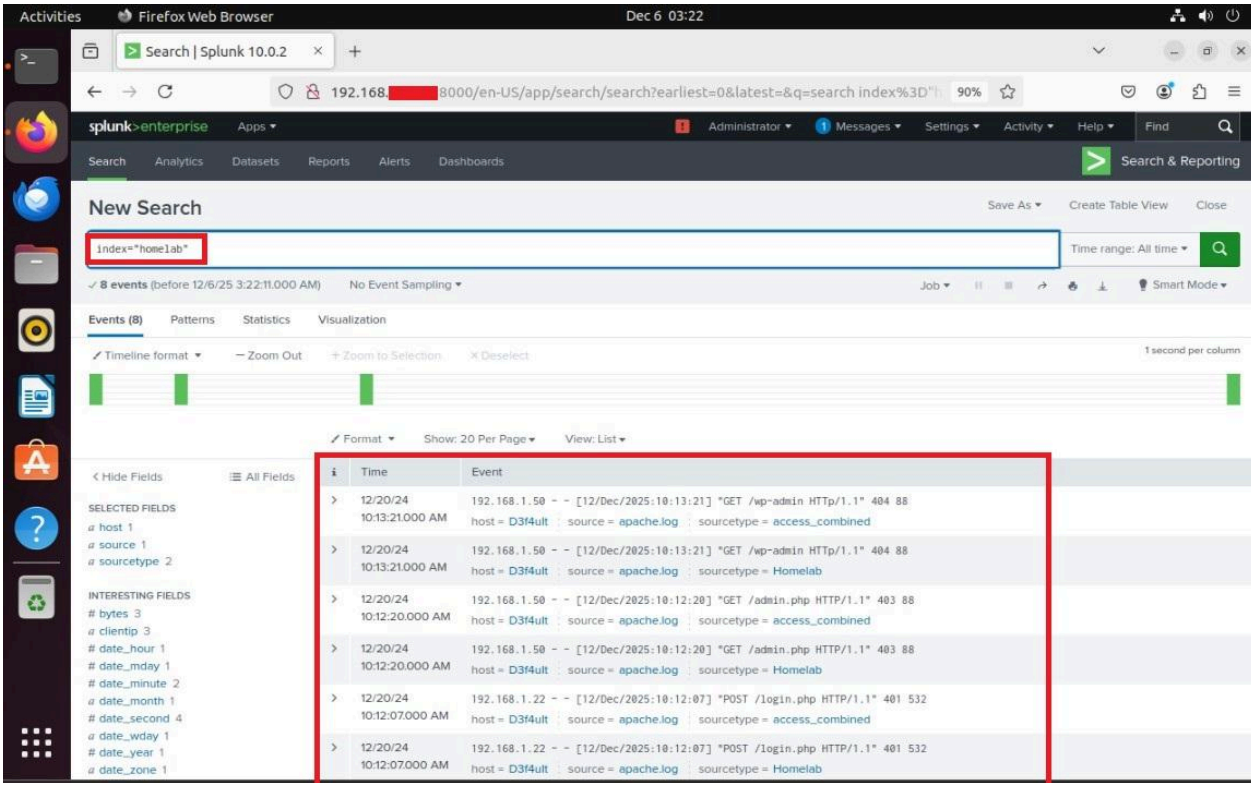
```
| eventcount summarize=false index=*
| sort - eventcount
```

Events by sourcetype:

```
index=*
| stats count by sourcetype
```

If you used a specific index name (example: `security_lab`), you can run:

```
index=security_lab | stats count by host, sourcetype
```



```
192.168.[redacted]8000/en-US/app/search/search?earliest=0&latest=&q=search index%3D"h
```

```
index="homelab"
```

✓ 8 events (before 12/6/25 3:22:11.000 AM)

```
Time                  Event
12/20/24              192.168.1.50 - - [12/Dec/2025:10:13:21] "GET /wp-admin HTTp/1.1" 404 88
10:13:21.000 AM       host = D3f4ult   source = apache.log   sourcetype = access_combined
12/20/24              192.168.1.50 - - [12/Dec/2025:10:13:21] "GET /wp-admin HTTp/1.1" 404 88
10:13:21.000 AM       host = D3f4ult   source = apache.log   sourcetype = Homelab
12/20/24              192.168.1.50 - - [12/Dec/2025:10:12:20] "GET /admin.php HTTP/1.1" 403 88
10:12:20.000 AM       host = D3f4ult   source = apache.log   sourcetype = access_combined
12/20/24              192.168.1.50 - - [12/Dec/2025:10:12:20] "GET /admin.php HTTP/1.1" 403 88
10:12:20.000 AM       host = D3f4ult   source = apache.log   sourcetype = Homelab
12/20/24              192.168.1.22 - - [12/Dec/2025:10:12:07] "POST /login.php HTTP/1.1" 401 532
10:12:07.000 AM       host = D3f4ult   source = apache.log   sourcetype = access_combined
12/20/24              192.168.1.22 - - [12/Dec/2025:10:12:07] "POST /login.php HTTP/1.1" 401 532
10:12:07.000 AM       host = D3f4ult   source = apache.log   sourcetype = Homelab
```

---

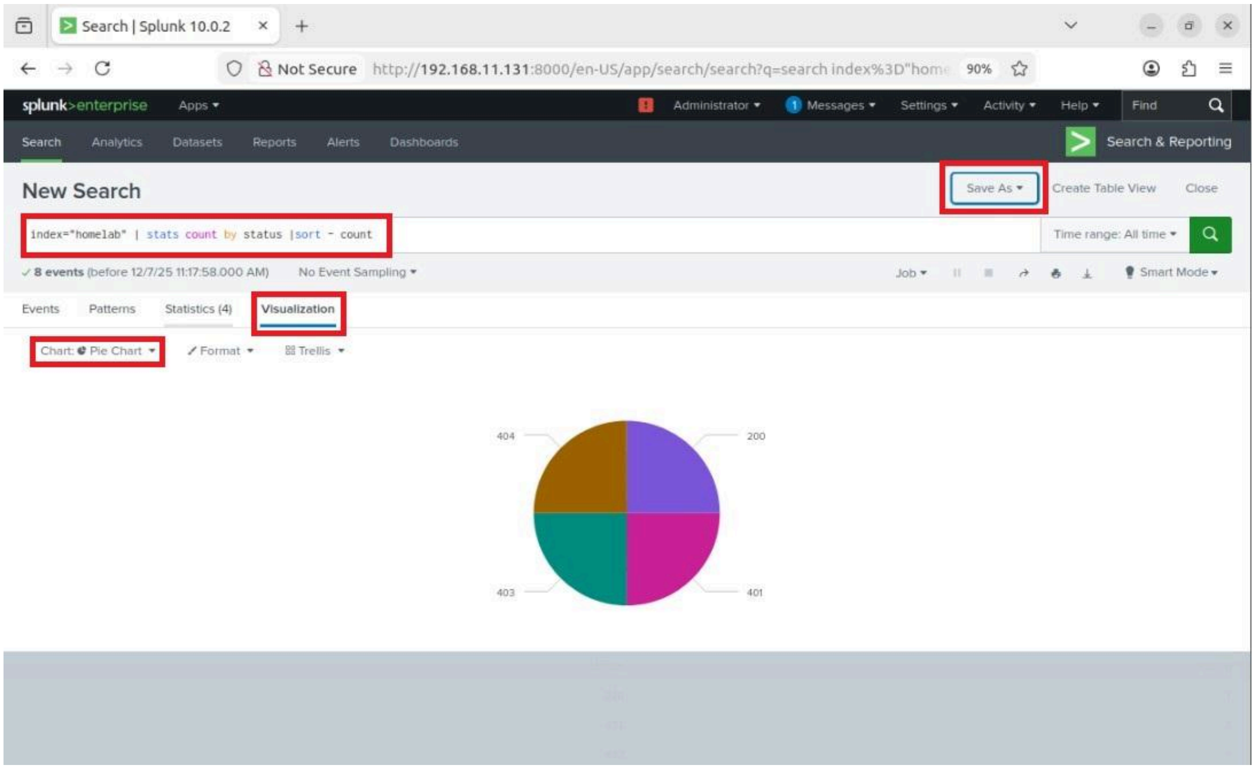
8. Create Simple Visualizations & Dashboards

To turn the searches into something more visual:

1. Ran a search like:

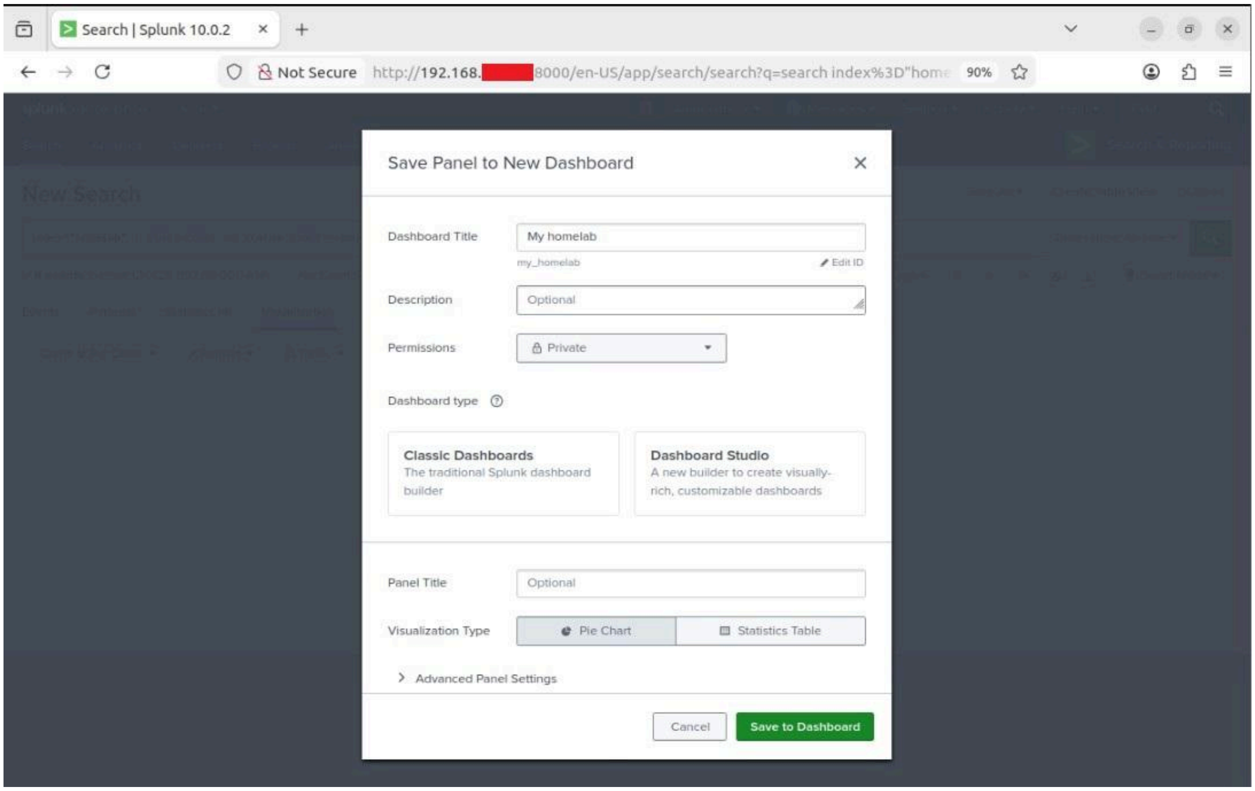
```
    index=homelab
| stats count by clientip
```

2. Clicked on **Visualization** and chose **Bar Chart / Pie Chart**
3. Saved it as a **Dashboard Panel**:
   - **Save As ➜ Dashboard Panel**
   - Created a new dashboard like My_homelab



```
index="homelab" | stats count by status |sort - count
```

✓ 8 events (before 12/7/25 11:17:58.000 AM)



Search | Splunk 10.0.2
Not Secure
http://192.168.[redacted]8000/en-US/app/search/search?q=search index%3D"home
90%
Save Panel to New Dashboard
Dashboard type
Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio
A new builder to create visually-rich, customizable dashboards
Advanced Panel Settings
Cancel
Save to Dashboard

Dashboard Title: My homelab

my_homelab ✎ Edit ID

Description: Optional

Permissions: Private ▾

Panel Title: Optional

Visualization Type: ● Pie Chart | Statistics Table

Repeated with another search, e.g.:

Top HTTP status codes:

```
index=homelab
| stats count by status
| sort - count
```

Events over time:

```
index=homelab
| timechart count by sourcetype
```

Added these to the same dashboard to have a small **SOC-style overview**.

---

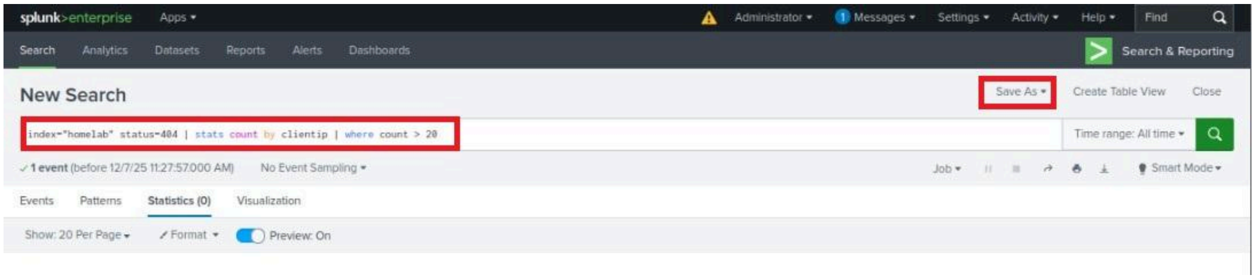
9. Created a Basic Alert

To simulate alerting:

Created a search for suspicious behavior (example):

1.
```
index=homelab status=404
| stats count by src_ip
| where count > 50
```

1.
2. Clicked **Save As ➜ Alert**



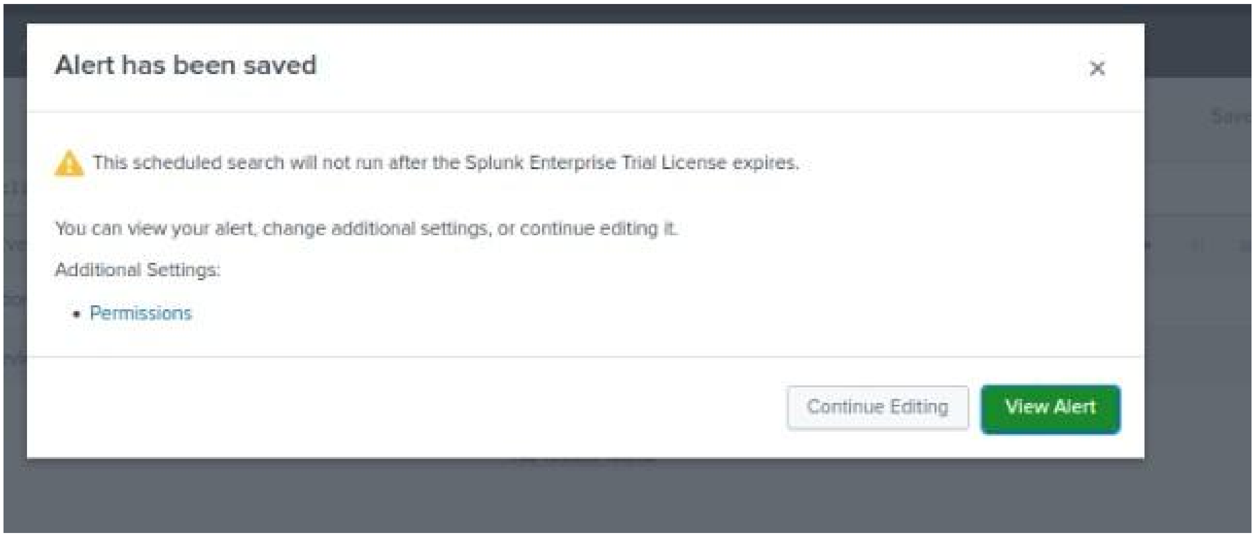
```
index="homelab" status=404 | stats count by clientip | where count > 20
```

✓ 1 event (before 12/7/25 11:27:57.000 AM)

3. Set:

   ○ Trigger: `if number of results > 0`

- ○ Schedule: e.g., `Every 5 minutes`
- ○ Action: `Add to Triggered Alerts`



Alert has been saved

⚠ This scheduled search will not run after the Splunk Enterprise Trial License expires.

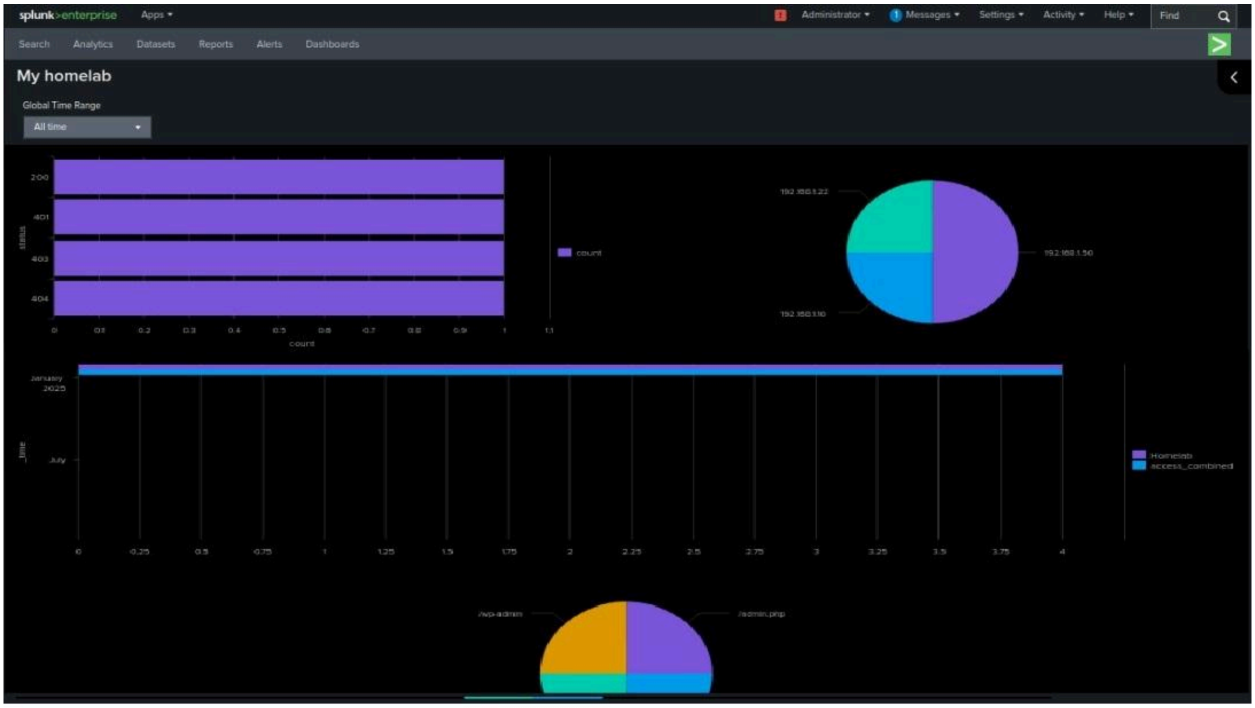
You can view your alert, change additional settings, or continue editing it.

Additional Settings:

- Permissions

This helped me understand how SOC teams configure rules and alerts in a SIEM.

After editing the Splunk dashboard and applying the desired changes, this is the final version I created:



10. What I Learned

From this homelab, I practiced:

- Installing and managing **Splunk on Ubuntu**
- Understanding **indexes, sourcetypes, and events**
- Writing basic **SPL (Search Processing Language)** queries
- Creating **dashboards** and **visualizations**
- Setting up simple **alerts** for security use cases

Next Steps

I plan to:

- Add more **log sources** (Windows logs, firewall logs, etc.)
- Build **detection use cases** (brute force, port scans, failed logins)
- Document the entire workflow and convert it into a **portfolio project**