

HOW TO INSTALL

**Ubuntu And Host a website with the help
of MySQL, MariaDB, PHP and Apache2**

HOW TO CONFIGURE

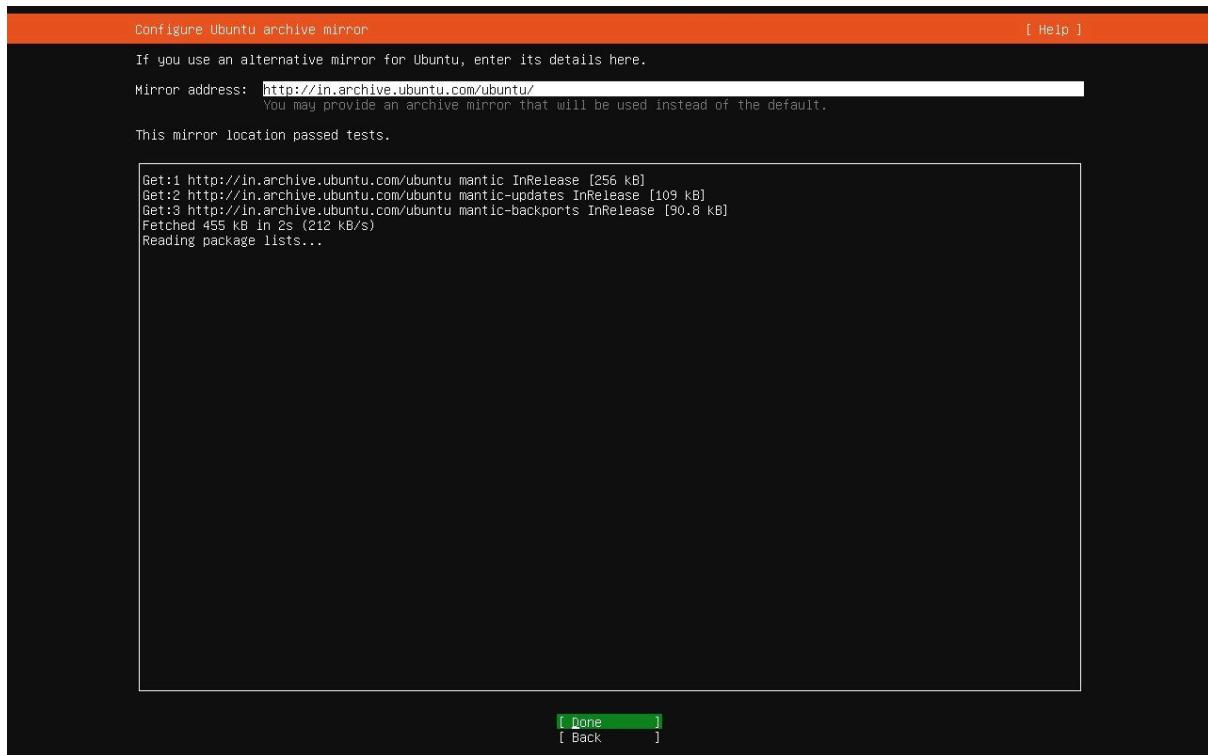
**Splunk Universal Forwarder on Ubuntu
and Monitor Website Logs**

Prepared by,

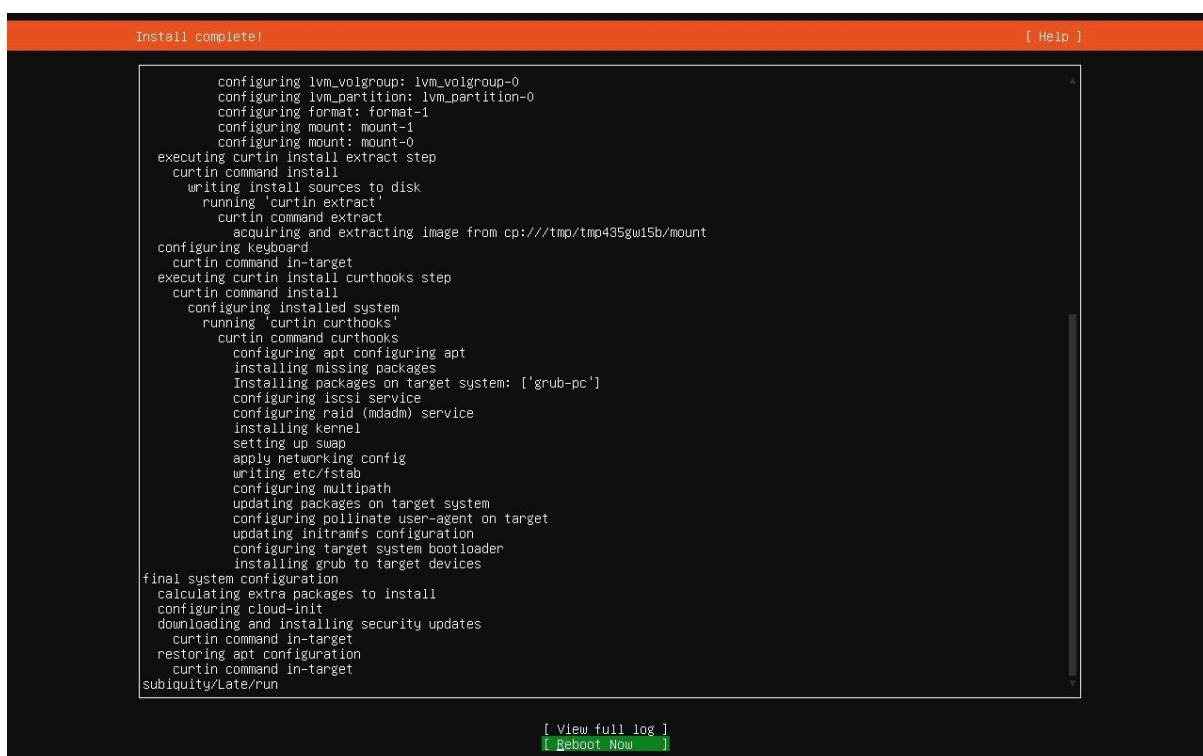
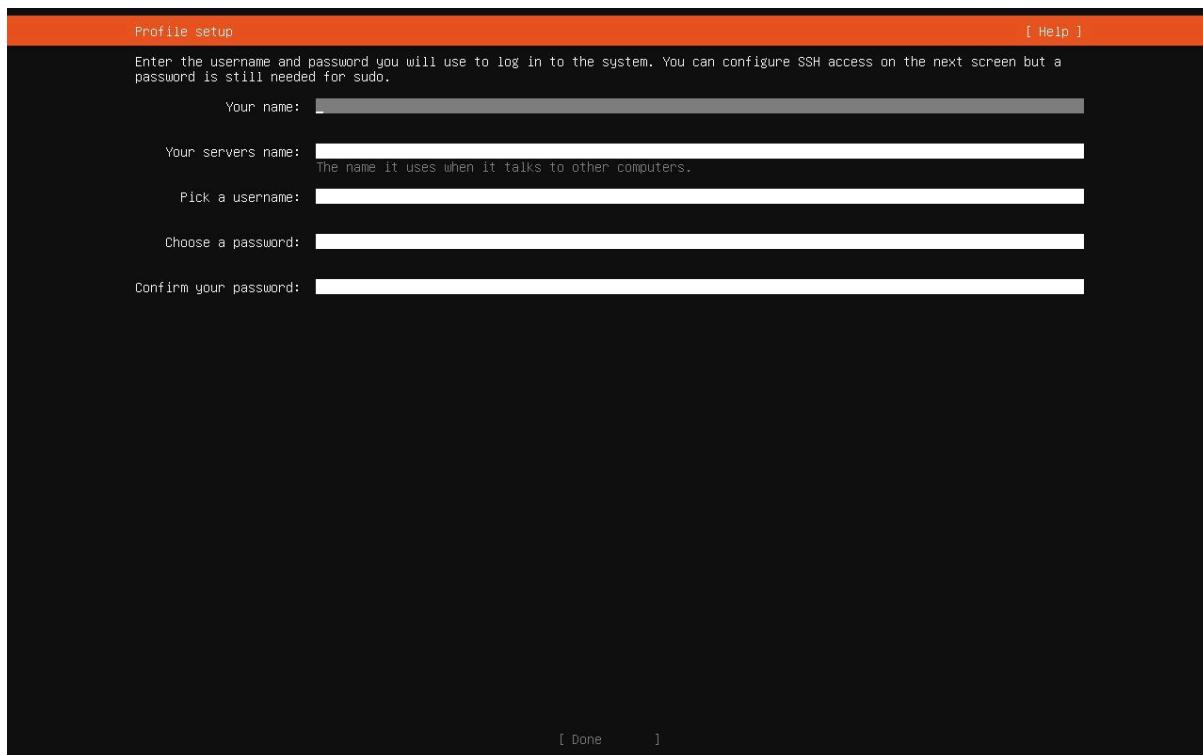
Athira V, Ramki Krishnan M R, Syam Babu

1. Steps to install Ubuntu Server

Download ubuntu server 22.04 . Install and configure a virtual machine in virtual box. Open Ubuntu and lets start it and install now.



Give your name ; server name ; username ; password



Ubuntu Installation is completed. The Ubuntu system terminal page is open and login with our username and password.

```
Ubuntu 23.10 krish tty1
krish login: ramki
Password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-15-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Mon Feb 5 03:26:25 PM UTC 2024

System load: 1.11      Processes: 119
Usage of /: 18.8% of 11.21GB  Users logged in: 0
Memory usage: 3%          IPv4 address for enp0s3: 192.168.18.145
Swap usage: 0%

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ramki@krish:~$
```

Step 2: Install Apache

Open the terminal on your Ubuntu system. The terminal is a text interface to your computer, which you will use to run all the commands.

First, update your software package list.

```
ramki@krish:~$ sudo apt-get update
```

```
ramki@krish:~$ sudo apt-get update
[sudo] password for ramki:
Hit:1 http://in.archive.ubuntu.com/ubuntu mantic InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu mantic-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu mantic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu mantic-security InRelease
Reading package lists... Done
ramki@krish:~$
```

The next step in setting up the LAMP stack will be installing and configuring Apache2, the web server. Run the below command to install Apache 2 on Ubuntu.

```
ramki@krish:~$ sudo apt install apache2
```

```
Last login: Tue Feb  6 14:43:58 2024
ramki@krish:~$ sudo apt install apache2
[sudo] password for ramki:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
    libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
    libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 41 not upgraded.
Need to get 2,097 KB of archives.
After this operation, 8,130 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

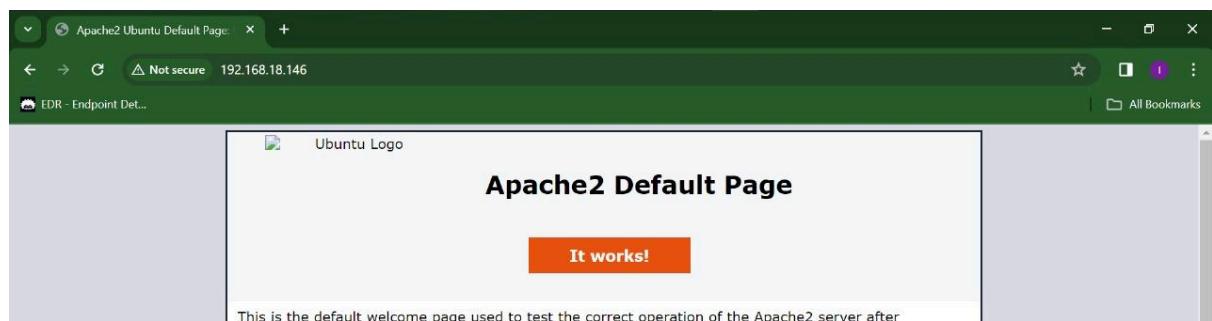
It is necessary to allow Apache2 to start at the system boot time and to start the service to verify its status as well.

```
ramki@krish:~$ sudo systemctl enable apache2
```

```
ramki@krish:~$ sudo systemctl status apache2
```

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
ramki@krish:~$ sudo systemctl enable apache2  
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable apache2  
ramki@krish:~$ sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)  
   Active: active (running) since Tue 2024-02-06 14:47:37 UTC; 2min 26s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
       Main PID: 1562 (apache2)  
         Tasks: 55 (limit: 7580)  
        Memory: 5.1M  
          CPU: 96ms  
        CGroup: /system.slice/apache2.service  
                 └─1562 /usr/sbin/apache2 -k start  
                   ├─1563 /usr/sbin/apache2 -k start  
                   ├─1564 /usr/sbin/apache2 -k start  
  
Feb 06 14:47:37 krish systemd[1]: Starting apache2.service - The Apache HTTP Server...
```

Open your web browser, and type localhost in the address box to verify that the Apache server has been started. If the Apache2 web server is running, it will display the default Apache2 index page



STEP 3: Installing MariaDB

Using the following command

```
ramki@krish:~$ sudo apt install mariadb-server mariadb-client
E: Invalid operation install
ramki@krish:~$ sudo apt install mariadb-server mariadb-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Reading state information... Done
E: Unable to locate package mariadb-client
ramki@krish:~$ sudo apt install mariadb-server mariadb-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
galera-4 libcgifast-perl libclone-perl libconfig-inifiles-perl libdaxctl libdbd-mysql-perl libdbi-perl libencode-locale-perl libfcgi-bin
libfcgi-perl libfcgi0ldbl libhtml-parser-perl libhtml-tagset-perl libhttp-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl
liblwp-mediatypes-perl libmariadb3 libmysqlclient21 libndctl16 libpmem1 libsnappyv5 libtimedate-perl liburi-perl liburing2 mariadb-client-core
mariadb-common mariadb-plugin-provider-bzrp2 mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
mariadb-plugin-provider-snappy mariadb-server-core mysql-common pv socat
Suggested packages:
libmldbm-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl libipc-sharedcache-perl libio-compress-brotli-perl libbusiness-isbn-perl
librexp-ipv6-perl libwww-mailx mariadb-test doc-base
The following NEW packages will be installed:
```

After checking the status of MariaDB services

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ramki@krish:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
ramki@krish:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-02-06 14:47:37 UTC; 2min 26s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 1562 (apache2)
      Tasks: 55 (limit: 7580)
     Memory: 5.1M
        CPU: 96ms
       CGroup: /system.slice/apache2.service
           ├─1562 /usr/sbin/apache2 -k start
           ├─1563 /usr/sbin/apache2 -k start
           └─1564 /usr/sbin/apache2 -k start
Feb 06 14:47:37 krish systemd[1]: Starting apache2.service - The Apache HTTP Server...

```

We enable MariaDB services

```
Feb 06 15:15:52 krish systemd[1]: Started mariadb.service - MariaDB 10.11.6 database server.
Feb 06 15:15:52 krish /etc/mysql/debian-start[2711]: Checking for insecure root accounts.
Feb 06 15:15:52 krish /etc/mysql/debian-start[2715]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria tables
ramki@krish:~$ sudo systemctl is-enabled mariadb.service
enabled
ramki@krish:~$ sudo mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.
```

STEP 4: Installing MYSQL, after complete installation we install PHP package.

Installing PHP packages.



```
ramki@krish: ~
Reload privilege tables now? [Y/n] y
... Success!
Cleaning up...
All done! If you've completed all of the above steps, your MariaDB installation should now be secure.

Thanks for using MariaDB!
ramki@krish:~$ sudo apt install php libapache2-mod-php php-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php8.2 php-common php8.2 php8.2-cli php8.2-common php8.2-mysql php8.2-opcache php8.2-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php libapache2-mod-php8.2 php php-common php-mysql php8.2 php8.2-cli php8.2-common php8.2-mysql php8.2-opcache php8.2-readline
0 upgraded, 4 newly installed, 0 to remove and 4 not upgraded.
```

After that we restart Apache2



```
athira@anant:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.184  netmask 255.255.255.0  broadcast 192.168.0.255
                inet6 fe80::a00:27ff:fe89:51b8  prefixlen 64  scoped_id 0x20<link>
        ether 08:00:27:89:51:b8  txqueuelen 1000  (Ethernet)
        RX packets 20701  bytes 27926760 (27.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7708  bytes 804887 (804.8 KB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                inet6 ::1  prefixlen 128  scope_id 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 152  bytes 14620 (14.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 152  bytes 14620 (14.6 KB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

athira@anant:~$ sudo systemctl restart apache2
athira@anant:~$ sudo vim /var/www/html/info.php
athira@anant:~$ 
```



```
athira@anant:~$ curl http://127.0.0.1/info.php
<!DOCTYPE html>
<html>
<head>
<title>PHP Information</title>
</head>
<body>
<pre>phpinfo();</pre>
</body>
</html>
```

Open your web browser, and type localhost /info.php in the address box to verify that the php has been started.

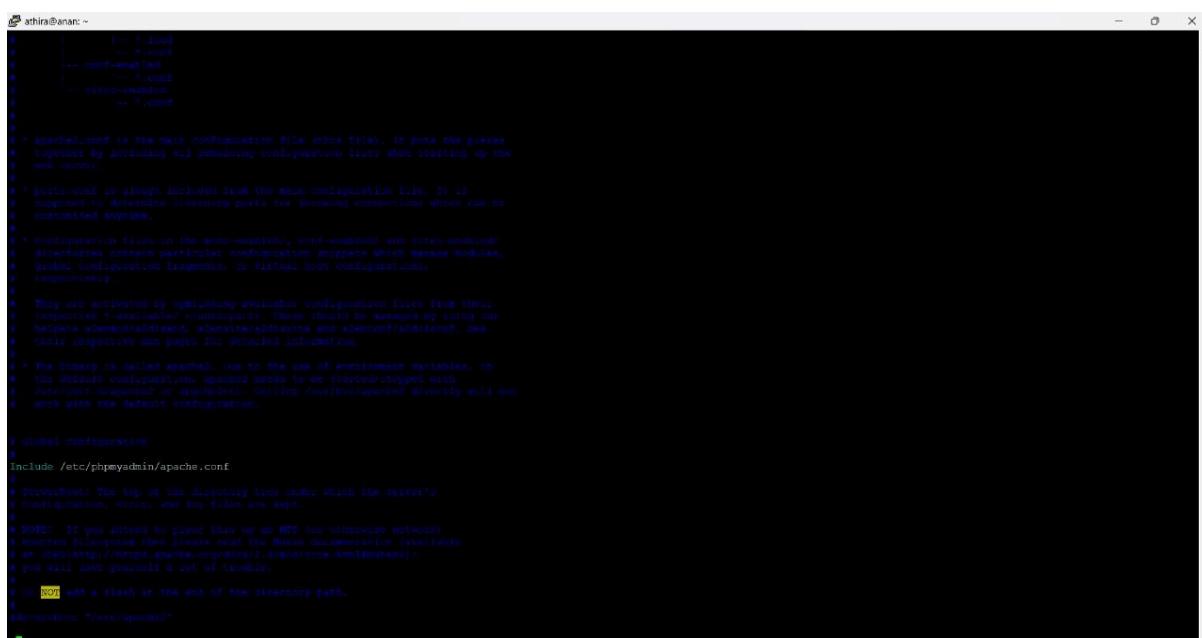
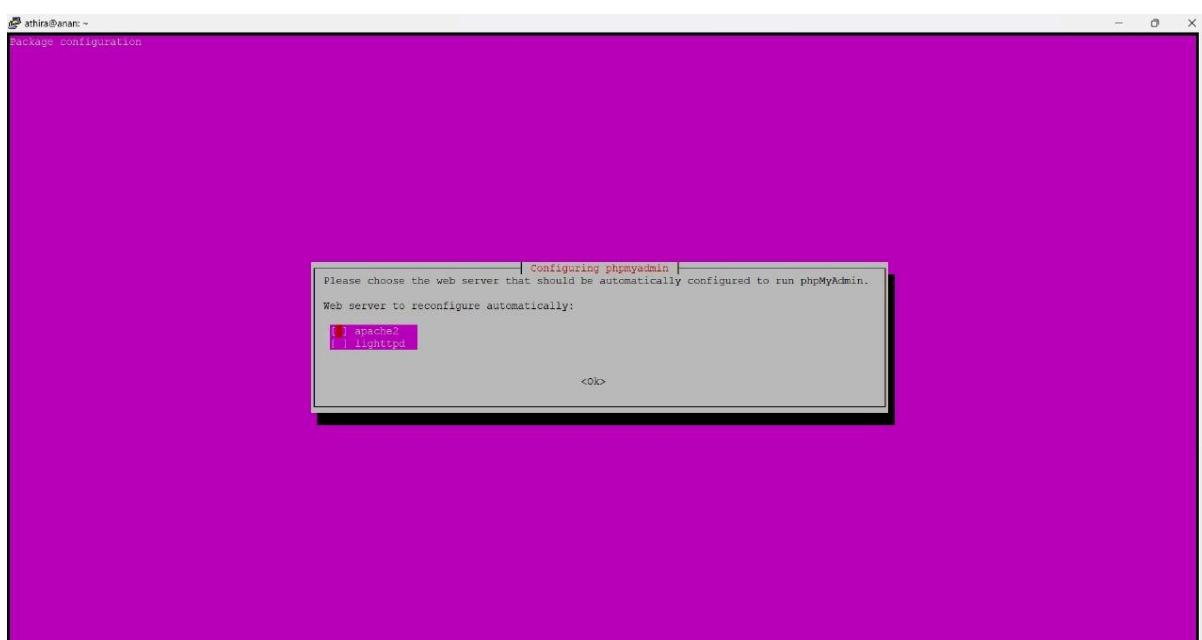
The screenshot shows a web browser window with the URL "192.168.0.184/info.php". The page title is "PHP Version 8.2.10-2ubuntu1". The content is a table of PHP configuration information. The table includes sections for System, Build Date, Build System, Server API, Virtual Directory Support, Configuration File (php.ini) Path, Loaded Configuration File, Scan this dir for additional .ini files, Additional .ini files parsed, PHP API, PHP Extension, Zend Extension, Zend Extension Build, PHP Extension Build, Debug Build, Thread Safety, Zend Signal Handling, Zend Memory Manager, Zend Multibyte Support, Zend Max Execution Timers, and Internal Server Errors. The table has a light blue header and white rows with black text.

PHP Version 8.2.10-2ubuntu1	
System	Linux anan 6.5.0-17-generic #17-Ubuntu SMP PREEMPT_DYNAMIC Thu Jan 11 14:01:59 UTC 2024 x86_64
Build Date	Sep 5 2023 14:37:47
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.2/apache2
Loaded Configuration File	/etc/php/8.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.2/apache2/conf.d
Additional .ini files parsed	/etc/php/8.2/apache2/conf.d/10-mysqli.ini, /etc/php/8.2/apache2/conf.d/10-opcache.ini, /etc/php/8.2/apache2/conf.d/10-pdo.ini, /etc/php/8.2/apache2/conf.d/10-pdo_mysql.ini, /etc/php/8.2/apache2/conf.d/10-pdo_sqlite.ini, /etc/php/8.2/apache2/conf.d/20-compress.ini, /etc/php/8.2/apache2/conf.d/20-curl.ini, /etc/php/8.2/apache2/conf.d/20-fpm.ini, /etc/php/8.2/apache2/conf.d/20-mbstring.ini, /etc/php/8.2/apache2/conf.d/20-mysqli.ini, /etc/php/8.2/apache2/conf.d/20-pdo_dblib.ini, /etc/php/8.2/apache2/conf.d/20-pecl.ini, /etc/php/8.2/apache2/conf.d/20-phar.ini, /etc/php/8.2/apache2/conf.d/20-pspell.ini, /etc/php/8.2/apache2/conf.d/20-readline.ini, /etc/php/8.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.2/apache2/conf.d/20-sysvsem.ini, /etc/php/8.2/apache2/conf.d/20-sysvshm.ini, /etc/php/8.2/apache2/conf.d/20-tokenizer.ini
PHP API	20220829
PHP Extension	20220829
Zend Extension	420220629
Zend Extension Build	APR20220829 NTS
PHP Extension Build	APR20220829 NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
Zend Max Execution Timers	disabled
Internal Server Errors	disabled

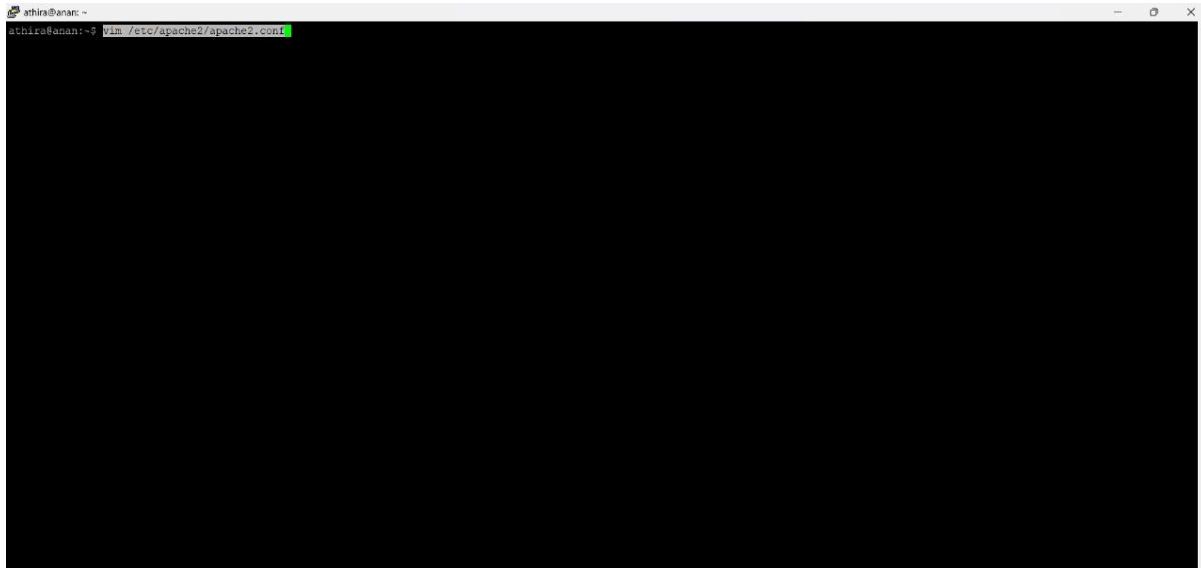
STEP 5: Installing PhP Admin



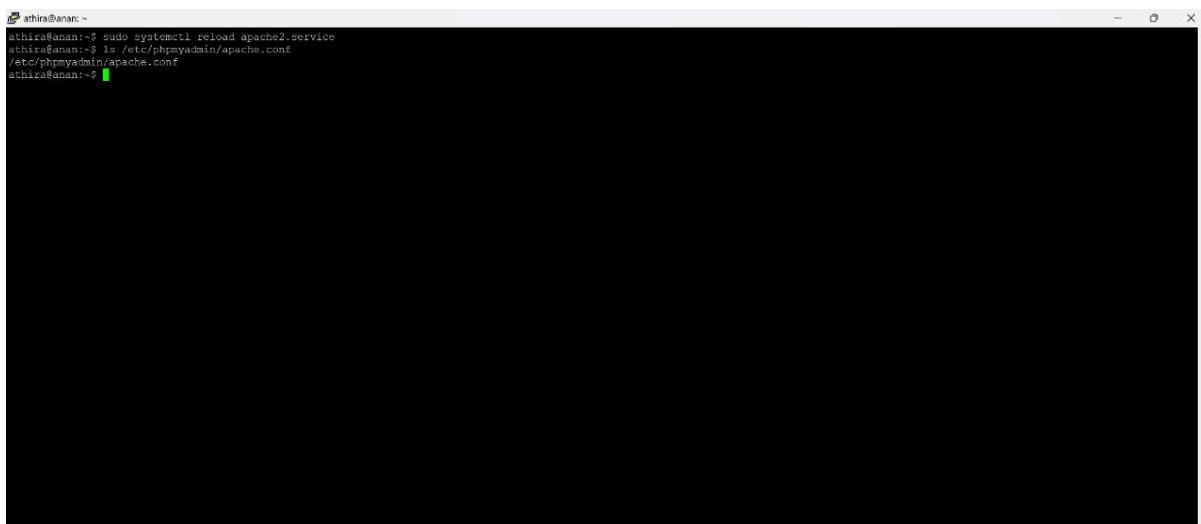
Then we do these configurations as done below in php admin



```
athira@anan:~  
athira@anan:~$ vim /etc/apache2/apache2.conf
```

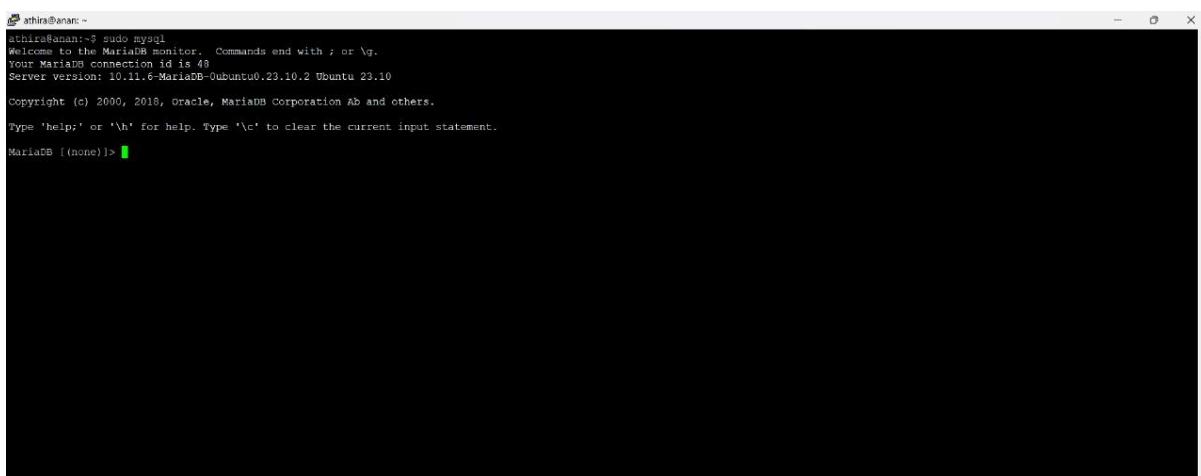


```
athira@anan:~  
athira@anan:~$ sudo systemctl reload apache2.service  
athira@anan:~$ ls /etc/phpmyadmin/apache.conf  
/etc/phpmyadmin/apache.conf  
athira@anan:~$
```



using admin rights to get sudo mysql

```
athira@anan:~  
athira@anan:~$ sudo mysql  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 48  
Server version: 10.11.6-MariaDB-0ubuntu0.23.10.2 Ubuntu 23.10  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
Type 'help' or '\h' for help. Type '\c' to clear the current input statement.  
MariaDB [(none)]>
```



```
athira@anant: ~
athira@anant: ~ $ sudo mysql
Welcome to the MariaDB monitor. Commands end with ; or \q.
Your MariaDB connection id is 50
Server version: 10.11.6-MariaDB-0ubuntu0.23.10.2 Ubuntu 23.10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE USER 'athira'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON . TO 'athira'@'localhost';
```

Adding database using my sql,Creating a user local identified by password.

Granting all privileges to the local user.

Pushing the privileges in to the db.

Exiting out of the database.

Restarting the Apache again.

```
ramki@krish: ~
Swap usage: 0%

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Thu Feb  8 09:28:55 2024 from 192.168.0.154
ramki@krish: ~ $ Sudo vim /etc/apache2/apache2.conf
Command 'Sudo' not found, did you mean:
  command 'ludo' from snap ludo (0.17.1)
  command 'ludo' from deb sudo (1.9.14p2-lubuntul)
  command 'sudo' from deb sudo-ldap (1.9.14p2-lubuntul)
  command 'udo' from deb udo (6.4.1-7)
See 'snap info <snapname>' for additional versions.
ramki@krish: ~ $ sudo vim /etc/apache2/apache2.conf
[sudo] password for ramki:
ramki@krish: ~ $ sudo vim /etc/apache2/apache2.conf
ramki@krish: ~ $ sudo mysql
Welcome to the MariaDB monitor. Commands end with ; or \q.
Your MariaDB connection id is 42
Server version: 10.11.6-MariaDB-0ubuntu0.23.10.2 Ubuntu 23.10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE USER 'ras'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.010 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON . TO 'ras'@'localhost';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'TO 'ras'@'localhost'' at line 1
MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'ras'@'localhost';
Query OK, 0 rows affected (0.010 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'FLUSH PRIVILEGES' at line 1
MariaDB [(none)]> FLUSH PRIVILEGES;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'FLUSH PRIVILEGES' at line 1
MariaDB [(none)]> FLUSH PRIVILEGES
    ->;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
```

Logging in to the PHP admin.



Making a media/shared directory.

Mounting the media directory.

```
athira@anan: ~
login as: athira
athira@192.168.0.184's password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-17-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Feb  8 09:49:06 AM UTC 2024

System load: 0.02      Processes:          107
Usage of /: 41.1% of 11.21GB  Users logged in: 1
Memory usage: 10%
Swap usage: 0%

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Thu Feb  8 10:43:55 2024
athira@anan:~$ sudo mkdir '/media/shared'
(sudo) password for athira:
athira@anan:~$ sudo mount -t vboxsf Webserve: /media/shared
```

```
athira@anan:/media/shared
└─ login as: athira
└─ athira@192.168.0.184's password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-17-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Feb  8 09:49:06 AM UTC 2024

System load: 0.02      Processes:          107
Usage of /: 41.1% of 11.21GB  Users logged in: 1
Memory usage: 10%      IPv4 address for enp0s3: 192.168.0.184
Swap usage:  0%

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Thu Feb  8 10:43:55 2024
athira@anan:~$ sudo mkdir /media/shared
[sudo] password for athira:
athira@anan:~$ sudo mount -t vboxsf Webserver /media/shared
athira@anan:~/media/shared$ ls
database.php index.php login.php logout.php registration.php style.css
athira@anan:~/media/shared$ sudo cp /media/shared/index.php /var/www/html/index.php
athira@anan:~/media/shared$ sudo cp /media/shared/login.php /var/www/html/login.php
athira@anan:~/media/shared$ sudo cp /media/shared/logout.php /var/www/html/logout.php
athira@anan:~/media/shared$ sudo cp /media/shared/style.css /var/www/html/style.css
athira@anan:~/media/shared$ sudo cp /media/shared/database.php /var/www/html/database.php
athira@anan:~/media/shared$
```

Reload the apache again.

```
athira@anan:~
└─ login as: athira
└─ athira@192.168.0.184's password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-17-generic x86_64)

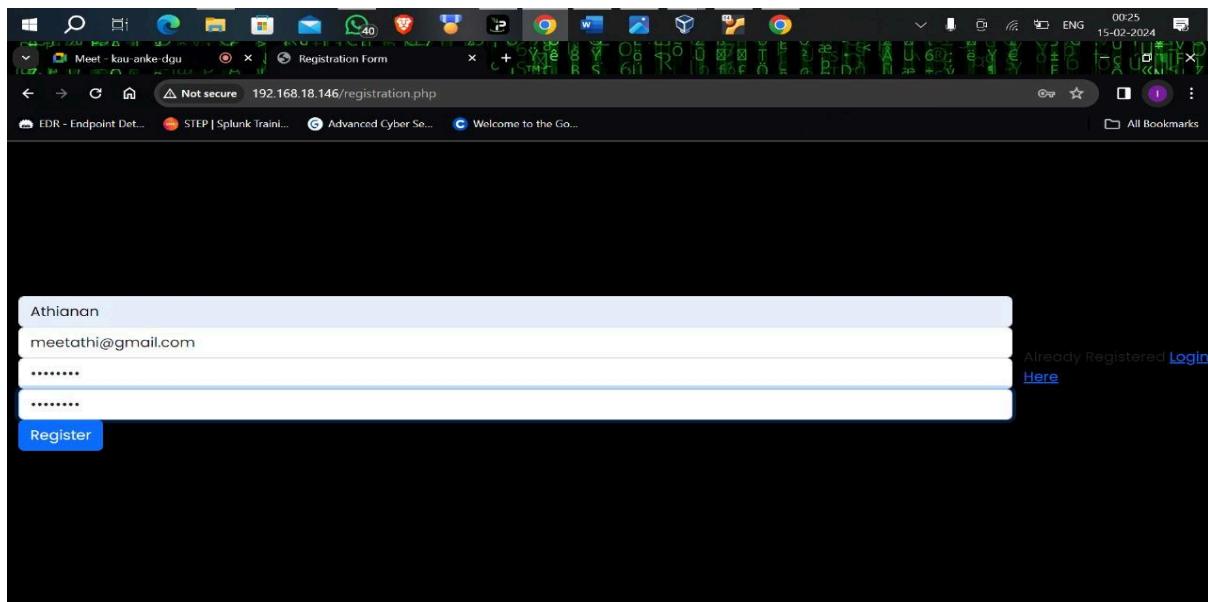
 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Feb  8 09:49:06 AM UTC 2024

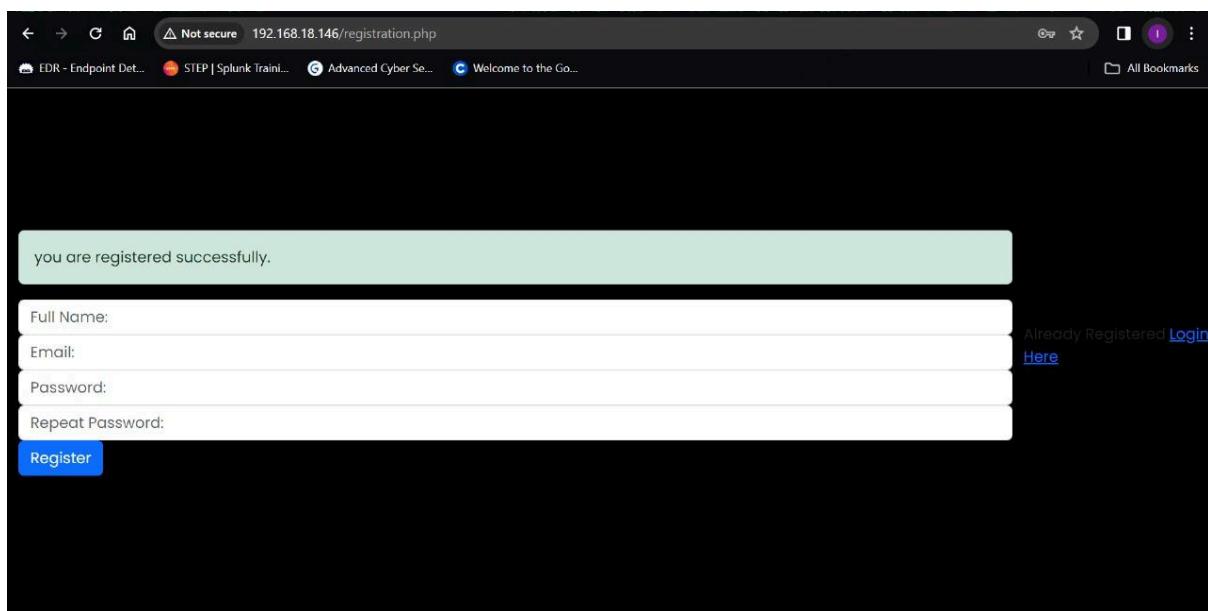
System load: 0.02      Processes:          107
Usage of /: 41.1% of 11.21GB  Users logged in: 1
Memory usage: 10%      IPv4 address for enp0s3: 192.168.0.184
Swap usage:  0%

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

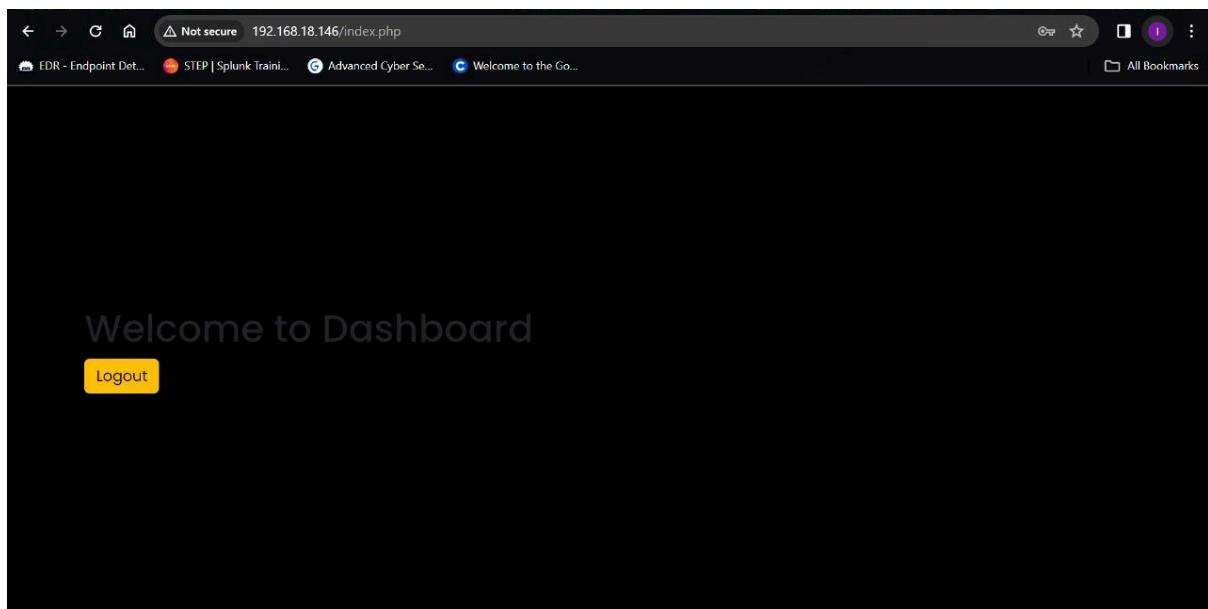
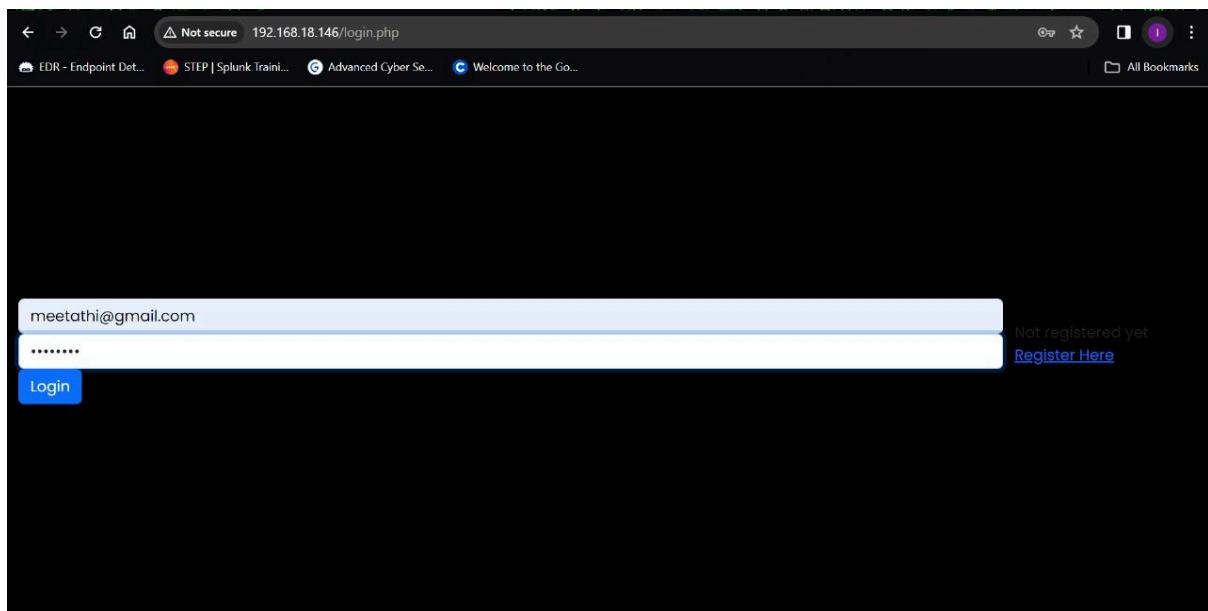
Last login: Thu Feb  8 10:43:55 2024
athira@anan:~$ sudo mkdir /media/shared
[sudo] password for athira:
athira@anan:~$ sudo mount -t vboxsf Webserver /media/shared
athira@anan:~/media/shared$ ls
database.php index.php login.php logout.php registration.php style.css
athira@anan:~/media/shared$ sudo cp /media/shared/index.php /var/www/html/index.php
athira@anan:~/media/shared$ sudo cp /media/shared/login.php /var/www/html/login.php
athira@anan:~/media/shared$ sudo cp /media/shared/logout.php /var/www/html/logout.php
athira@anan:~/media/shared$ sudo cp /media/shared/style.css /var/www/html/style.css
athira@anan:~/media/shared$ sudo cp /media/shared/database.php /var/www/html/database.php
athira@anan:~/media/shared$ cd /var/www/html
athira@anan:~/var/www/html$ ls
database.php index.php info.php login.php logout.php registration.php style.css
athira@anan:~/var/www/html$ sudo rm index.html
athira@anan:~/var/www/html$ ls
database.php index.php info.php login.php logout.php registration.php style.css
athira@anan:~/var/www/html$ cd
athira@anan:~$ sudo systemctl restart apache2
athira@anan:~$ sudo systemctl reload apache2
athira@anan:~$
```



Registering into the PHP server

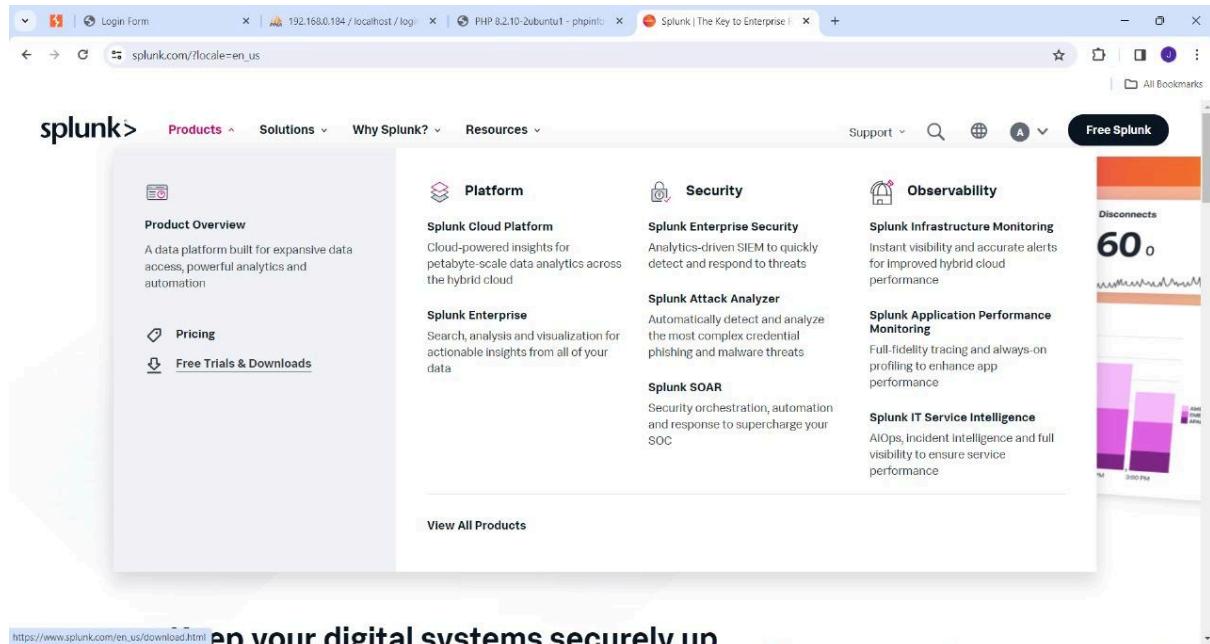


Logging into the server.



STEP 6: Splunk Universal Forwarder Installation

We can begin installing splunk forwarder.First,we will download the splunk forwarder installation file.



Steps to find universal forwarder Download via command

1. *Free Splunk*
2. *Free trials and downloads*
3. *Universal Forwarder*
4. *Linux*
5. *64-bit.tgz*

Click the Command Line (wget) and copy it

The screenshot shows a web browser window with multiple tabs open. The active tab is 'splunk.com/en_us/download.html'. The page content is for the 'Universal Forwarder' product. It features a large orange and yellow graphic with binary code (0010, 01010, 0101) and a small network icon. Below the graphic, there's a button labeled 'Get My Free Download'.

Type wget and the copied link into the terminal.

```
ahira@anan:~$ wget -O splunkforwarder-9.2.0-1fff80043d5f-Linux-x86_64.tgz "https://download.splunk.com/products/universalforwarder/releases/9.2.0/linux/splunkforwarder-9.2.0-1fff80043d5f-Linux-x86_64.tgz"
--2024-02-08 11:09:19-- https://download.splunk.com/products/universalforwarder/releases/9.2.0/linux/splunkforwarder-9.2.0-1fff80043d5f-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 18.161.216.62, 18.161.216.79, 18.161.216.90, ...
Connecting to download.splunk.com (download.splunk.com)|18.161.216.62|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4506681 (44Mi) [binary/octet-stream]
Saving to: 'splunkforwarder-9.2.0-1fff80043d5f-Linux-x86_64.tgz'

splunkforwarder-9.2.0-1fff80043d5f-Linux-x86_64 100%[=====] 43.68M  17.6MB/s   in 2.5s
2024-02-08 11:09:19 (17.6 MB/s) - 'splunkforwarder-9.2.0-1fff80043d5f-Linux-x86_64.tgz' saved [4506681/4506681]
ahira@anan:~$
```

Extract the splunk forwarder files to opt location

```
ahira@anan:~$ wget -O splunkforwarder-9.2.0-1fff88043d5f-Linux-x86_64.tgz "https://download.splunk.com/products/universalforwarder/releases/9.2.0/linux/splunkforwarder-9.2.0-1fff88043d5f-Linux-x86_64.tgz"
--2024-02-08 11:09:16-- https://download.splunk.com/products/universalforwarder/releases/9.2.0/linux/splunkforwarder-9.2.0-1fff88043d5f-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 18.161.216.62, 18.161.216.73, 18.161.216.90, ...
Connecting to download.splunk.com (download.splunk.com)|18.161.216.62|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45006681 [binary/octet-stream]
Saving to: 'splunkforwarder-9.2.0-1fff88043d5f-Linux-x86_64.tgz'

splunkforwarder-9.2.0-1fff88043d5f-Linux-x86_64 100%[=====] 43.60M 17.6MB/s   in 2.5s

2024-02-08 11:09:19 (17.6 MB/s) - 'splunkforwarder-9.2.0-1fff88043d5f-Linux-x86_64.tgz' saved [45006681/45006681]

ahira@anan:~$ sudo tar xfz splunkforwarder-9.2.0-1fff88043d5f-Linux-x86_64.tgz -C /opt
[sudo] password for ahira:
splunkforwarder/
splunkforwarder/swiftag/
splunkforwarder/swiftag/splunk-UniversalForwarder-primary.swiftag
splunkforwarder/ltc/
splunkforwarder/openssl/
splunkforwarder/openssl/misc/
splunkforwarder/openssl/misc/c_info
splunkforwarder/openssl/misc/tsgut
splunkforwarder/openssl/misc/c_issuer
splunkforwarder/openssl/misc/C_sh
splunkforwarder/openssl/misc/c_hash
splunkforwarder/openssl/misc/c_name
splunkforwarder/openssl/misc/C_A_p1
splunkforwarder/openssl/openssl.cnf
splunkforwarder/openssl/copyright.txt
splunkforwarder/share/
splunkforwarder/share/mongo-c-driver/
splunkforwarder/share/mongo-c-driver/uninstall.sh
splunkforwarder/share/mongo-c-driver/NEWS
splunkforwarder/share/mongo-c-driver/COPYING
splunkforwarder/share/mongo-c-driver/README.rst
splunkforwarder/share/mongo-c-driver/THIRD_PARTY_NOTICES
splunkforwarder/share/copyright.txt
splunkforwarder/share/splunk/
splunkforwarder/share/splunk/3rdparty/
splunkforwarder/share/splunk/3rdparty/copyright-for-ac.lockfile-2.0.txt
splunkforwarder/share/splunk/3rdparty/copyright-for-pcre2-10.40.txt
splunkforwarder/share/splunk/3rdparty/copyright-for-jemalloc-4.5.0.txt
splunkforwarder/share/splunk/3rdparty/copyright-for-prometheus-cpp-0.9.0.txt
splunkforwarder/share/splunk/3rdparty/copyright-for-setupools_scm_git_archive-1.1.txt
splunkforwarder/share/splunk/3rdparty/copyright-for-FormEncode-1.3.1.txt
splunkforwarder/share/splunk/3rdparty/copyright-for-hive-4.0.0-beta-1.txt
splunkforwarder/share/splunk/3rdparty/copyright-for-protocols-1.29.157.txt
splunkforwarder/share/splunk/3rdparty/copyright-for-double-conversion-3.0.0.txt
```

Change to opt directory

```
ahira@anan:/opt/splunkforwarder/bin$ ls
splunkforwarder/etc/users/users.ini.default
splunkforwarder/etc/manager-apps/
splunkforwarder/etc/manager-apps/_cluster/
splunkforwarder/etc/manager-apps/_cluster/local/
splunkforwarder/etc/manager-apps/_cluster/local/README
splunkforwarder/etc/manager-apps/_cluster/default/
splunkforwarder/etc/manager-apps/_cluster/default/indexes.conf
splunkforwarder/etc/log-bitool-debug.cfg
splunkforwarder/etc/modules/
splunkforwarder/etc/modules/parsing/
splunkforwarder/etc/modules/parsing/config.xml
splunkforwarder/etc/modules/input/
splunkforwarder/etc/modules/input/FIFO/
splunkforwarder/etc/modules/input/FIFO/config.xml
splunkforwarder/etc/modules/input/exec/
splunkforwarder/etc/modules/input/exec/config.xml
splunkforwarder/etc/modules/input/RemoteQueue/
splunkforwarder/etc/modules/input/RemoteQueue/config.xml
splunkforwarder/etc/modules/input/tailfile/
splunkforwarder/etc/modules/input/tailfile/config.xml
splunkforwarder/etc/modules/input/UDF/
splunkforwarder/etc/modules/input/UDF/config.xml
splunkforwarder/etc/modules/input/structuredparsing/
splunkforwarder/etc/modules/input/structuredparsing/config.xml
splunkforwarder/etc/modules/input/TCP/
splunkforwarder/etc/modules/input/TCP/config.xml
splunkforwarder/etc/modules/input/fchangemanager/
splunkforwarder/etc/modules/input/fchangemanager/config.xml
splunkforwarder/etc/modules/output/
splunkforwarder/etc/modules/output/config.xml
splunkforwarder/etc/modules/output/Remotequeue/
splunkforwarder/etc/modules/output/Remotequeue/config.xml
splunkforwarder/etc/schcluster/
splunkforwarder/etc/schcluster/apps/
splunkforwarder/etc/schcluster/apps/README
splunkforwarder/etc/schcluster/users/
splunkforwarder/etc/schcluster/users/README
splunkforwarder/etc/log-utility.cfg
splunkforwarder/etc/prettyprint.xml
splunkforwarder/etc/init.d/
splunkforwarder/etc/init.d/README
splunkforwarder/etc/init.d/splunk.conf.default
splunkforwarder/etc/log/cmdline.cfg
splunkforwarder/etc/deployment-apps/
splunkforwarder/etc/deployment-apps/README
splunkforwarder/etc/log-debug.cfg
ahira@anan:~$ cd /opt/splunkforwarder/bin
ahira@anan:/opt/splunkforwarder/bin$
```

ubuntu@ubuntu:/tmp\$ cd /opt

ubuntu@ubuntu:/opt\$ cd splunkforwarder/bin

```
athira@anan:/opt/splunkforwarder/bin
cd /opt/splunkforwarder/bin
athira@anan:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-license
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: admin
Password must contain at least:
    * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Failed to auto-set default user.
Failed to create the unit file. Please do it manually later.

Splunk> Finding your faults, just like mom.

Checking prerequisites...
    Checking mgmt port [8089]: open
        Creating: /opt/splunkforwarder/var/lib/splunk
        Creating: /opt/splunkforwarder/var/run/splunk
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
        Creating: /opt/splunkforwarder/var/run/splunk/upload
        Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
        Creating: /opt/splunkforwarder/var/run/splunk/search_log
        Creating: /opt/splunkforwarder/var/spool/splunk
        Creating: /opt/splunkforwarder/var/spool/dimoncache
        Creating: /opt/splunkforwarder/var/lib/splunk/authDb
        Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
    Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.2.0-1fff08043d5f-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONTLSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

athira@anan:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.0.193:9997
```

```
athira@anan:/opt/splunkforwarder/bin
cd /opt/splunkforwarder/bin
athira@anan:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-license
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: admin
Password must contain at least:
    * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Failed to auto-set default user.
Failed to create the unit file. Please do it manually later.

Splunk> Finding your faults, just like mom.

Checking prerequisites...
    Checking mgmt port [8089]: open
        Creating: /opt/splunkforwarder/var/lib/splunk
        Creating: /opt/splunkforwarder/var/run/splunk
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
        Creating: /opt/splunkforwarder/var/run/splunk/upload
        Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
        Creating: /opt/splunkforwarder/var/run/splunk/search_log
        Creating: /opt/splunkforwarder/var/spool/splunk
        Creating: /opt/splunkforwarder/var/spool/dimoncache
        Creating: /opt/splunkforwarder/var/lib/splunk/authDb
        Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
    Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.2.0-1fff08043d5f-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONTLSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

athira@anan:/opt/splunkforwarder/bin$
```

Step 7: Configuring Splunk Server

Configuring firewall in windows

When configuring the firewall for a Splunk server on Windows, you need to ensure that the necessary ports are open to allow communication between Splunk components. Splunk uses specific ports for different purposes, and you must adjust your Windows Firewall settings accordingly. Here are the general steps to configure the Windows Firewall for a Splunk server:

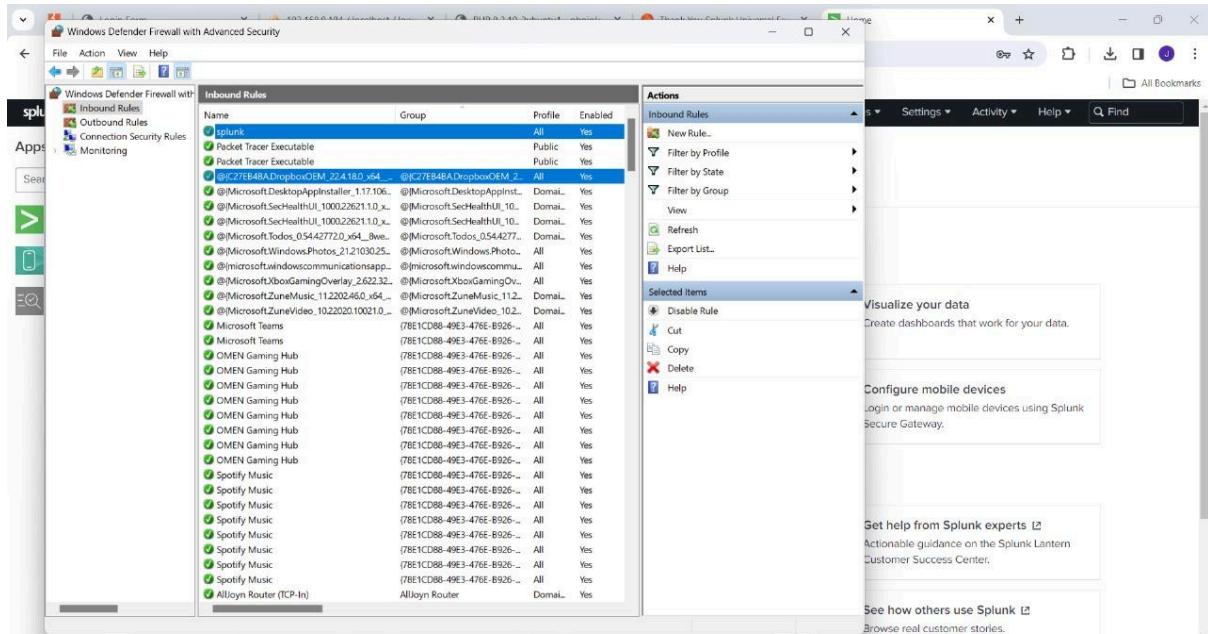
Open Windows Firewall Settings:

Go to the Control Panel on your Windows server.

Click on "System and Security" and then "Windows Defender Firewall."

Create Inbound Rules:

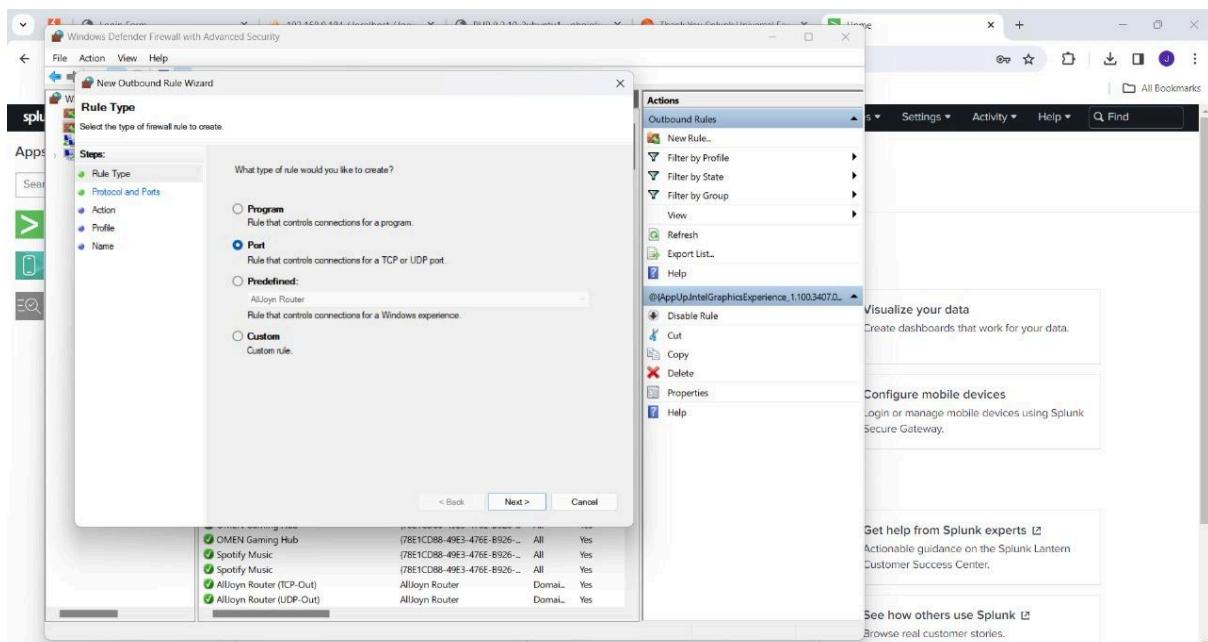
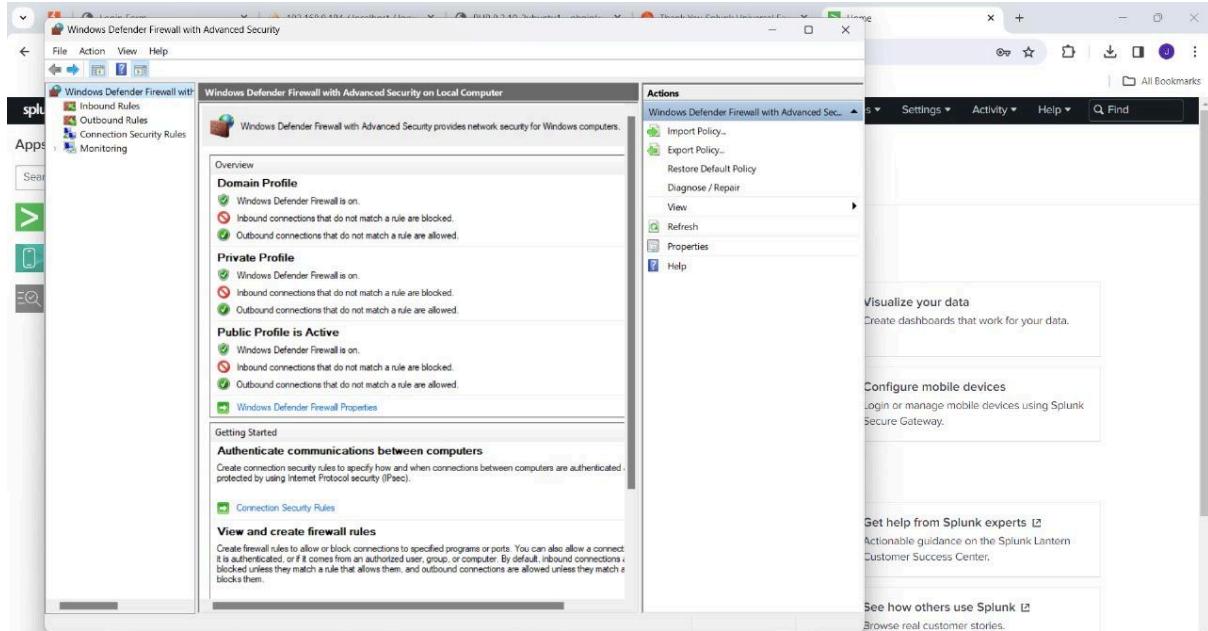
Click on "Advanced settings" on the left side



Configure Inbound Rules:

In the “Inbound Rules” section, click on “New Rule....” On the right side.

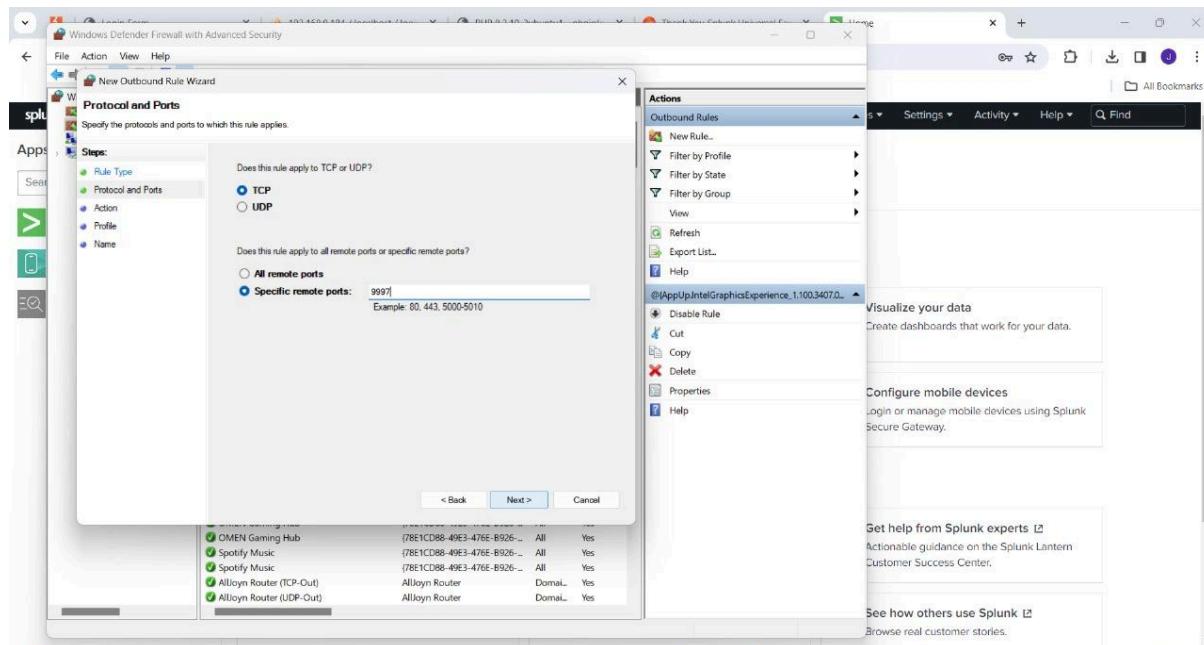
Select “port” and click “next”



Specify ports:

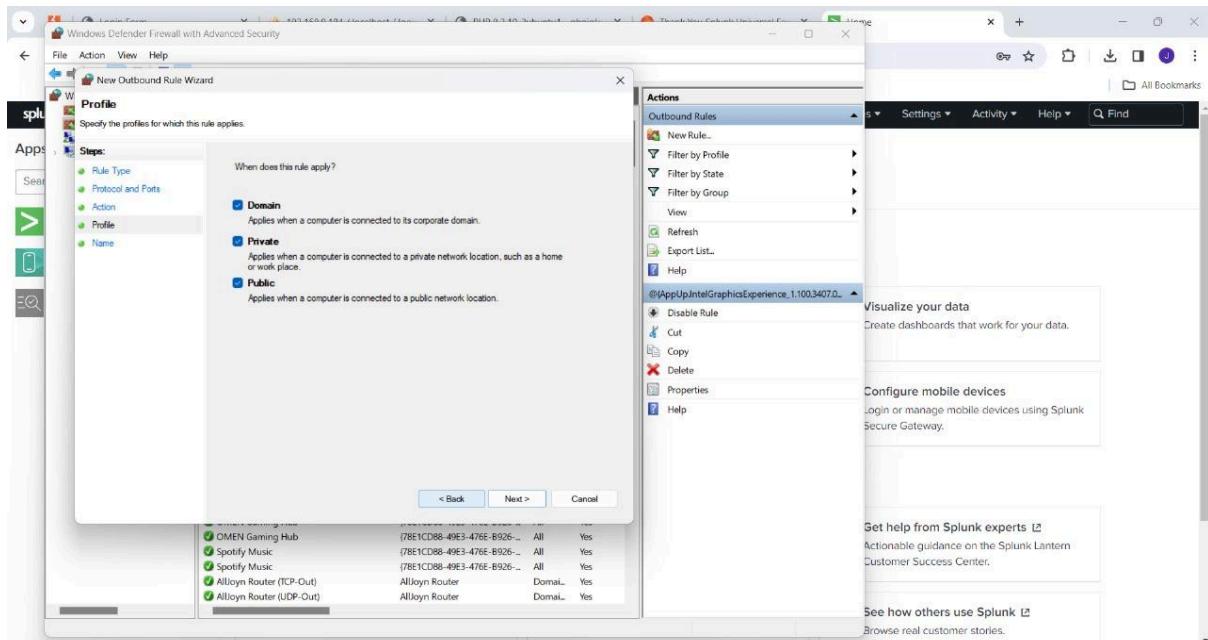
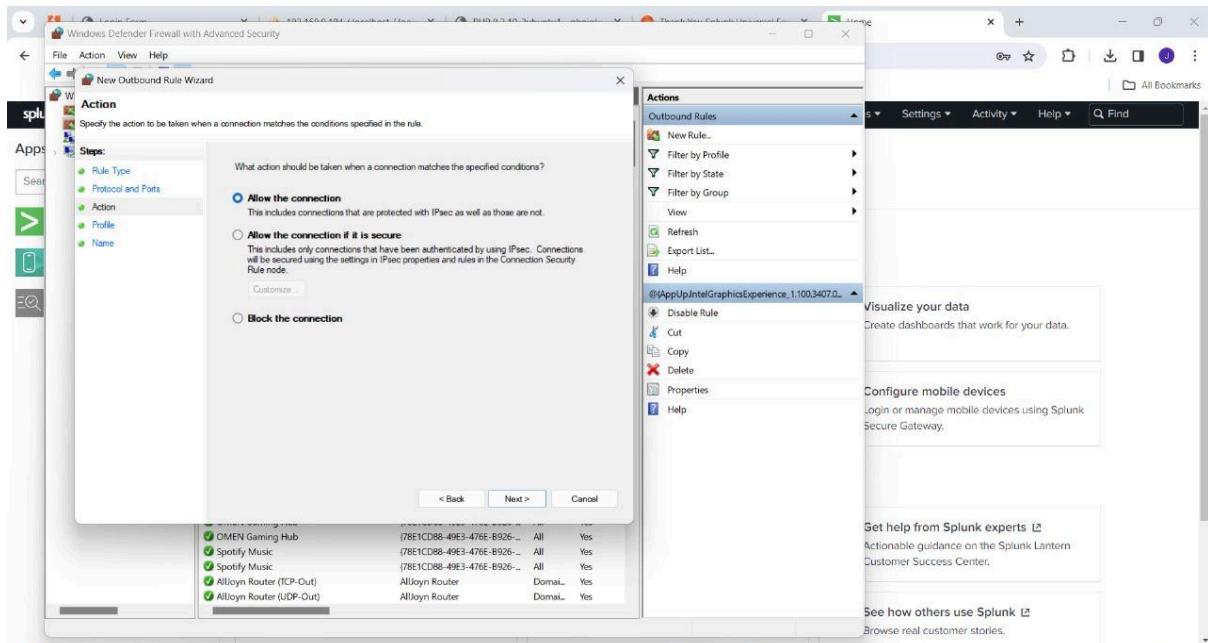
Choose “TCP” and specify the ports relevant to your splunk setup (e.g 9997).

Click “Next.”



Choose Action:

Select “allow the connection” and click “Next.”



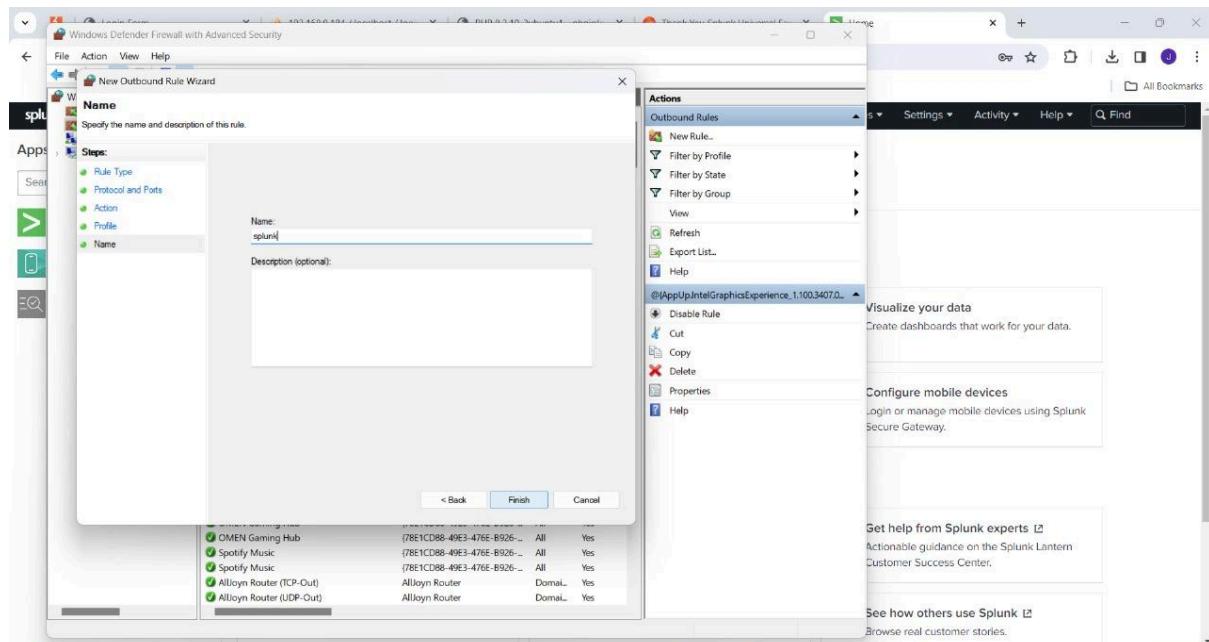
Profile settings:

Choose when to apply the rule based on your network profile settings (Domain, Private, Public).

Click "next."

Rule name:

Provide a name for the rule (e.g., splunk web interface)



Click "Finish."

Step 8 : Configuring Splunk Universal Forwarder

Configuring splunk forwarder on an Ubuntu server to monitor logs from windows machine.

```
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.2.0-1fff80043d5f-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
athira@man: /opt/splunkforwarder/bin$
```

Add this lines ;

[tcpout]

defaultGroup = splunk-group

[tcpout:splunk-group]

server = <splunk_server_ip>:<splunk_listener_port>

Replace server ip in here (windows machine ip) <splunk_server_ip> and give port number <splunk_listener_port> (eg; 9997).

```
athira@anan:/opt/splunkforwarder/bin
$ ./splunkforwarder/bin$ sudo ./splunk start --accept-license
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: admin
Password must contain at least:
    * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Failed to auto-set default user.
Failed to create the unit file. Please do it manually later.

Splunk> Finding your faults, just like mom.

Checking prerequisites...
    Checking mgmt port [8089]: open
        Creating: /opt/splunkforwarder/var/lib/splunk
        Creating: /opt/splunkforwarder/var/run/splunk
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/upload
        Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
        Creating: /opt/splunkforwarder/var/run/splunk/search_log
        Creating: /opt/splunkforwarder/var/spool/splunk
        Creating: /opt/splunkforwarder/var/spool/dimoncache
        Creating: /opt/splunkforwarder/var/lib/splunk/authDb
        Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
    Checking conf files for problems...
        Done.
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.2.0-1fff88043d5f-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done.
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONTLSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done.

athira@anan:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.0.103:9997
```

Adding forwarding and adding log monitoring and restarting.

```
athira@anan:/opt/splunkforwarder/bin
$ ./splunkforwarder/bin$ sudo ./splunk restart
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
.
Stopping splunk helpers...
.
Done.

Splunk> Finding your faults, just like mom.

Checking prerequisites...
    Checking mgmt port [8089]: open
    Checking conf files for problems...
        Done.
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.2.0-1fff88043d5f-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done.
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONTLSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done.

athira@anan:/opt/splunkforwarder/bin$
```

Step 9: Splunk enterprise configuration

To set up forwarding and receiving ports in Splunk, you'll typically configure the Universal

Forwarder to send data to the main Splunk Enterprise instance. Below are the general

steps to add forwarding and receiving ports in Splunk:

- v *Receiving Port (Splunk Enterprise): This port is used by Splunk Enterprise to listen for incoming data from Universal Forwarders.*
- v *Access Splunk Web: Open your web browser and navigate to the Splunk Web interface. Log in with appropriate credentials.*
- v *Navigate to Settings: In the Splunk Web interface, go to "Settings" in the top menu.*

Configure Receiving Port: Under "Settings," click on "Forwarding and Receiving." Click on "Configure receiving" and specify the receiving port (e.g., 9997). Save the configuration

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Hello, Administrator

Apps Manage

Search apps by name...

Quick links Dashboard Recently viewed Created by you Shared with you

Add Data

Common tasks

- Add data** Add data from a variety of common sources.
- Search your data** Turn data into doing with search.
- Add team members** Add your team members to Splunk platform.
- Manage permissions** Control who has access.

Learning and resources

- Product tours** New to Splunk? Take a tour to help you on your way.
- Learn more with Splunk Docs** Deploy, manage, and use Splunk software with comprehensive guidance.
- Get help from Splunk experts** Actionable guidance on the Splunk Lantern Customer Success Center.
- Extend your capabilities** Browse thousands of apps on Splunkbase.
- Join the Splunk Community** Learn, get inspired, and share knowledge.
- See how others use Splunk** Browse real customer stories.

DATA

SEARCHES, REPORTS, AND ALERTS
DATA INPUTS
DATA MODELS
FORWARDING AND RECEIVING
EVENT TYPES
INDEXES
TAGS
FIELDS
LOOKUPS
USER INTERFACE
ALERT ACTIONS
ADVANCED SEARCH
ALL CONFIGURATIONS

DISTRIBUTED ENVIRONMENT

INDEX CLUSTERING
FORWARDER MANAGEMENT
FEDERATED SEARCH
DISTRIBUTED SEARCH

SYSTEM

SERVER SETTINGS
SERVER CONTROLS
HEALTH REPORT MANAGER
INSTRUMENTATION
LICENSING
WORKLOAD MANAGEMENT
MOBILE SETTINGS

USERS AND AUTHENTICATION

ROLES
USERS
TOKENS
PASSWORD MANAGEMENT
AUTHENTICATION METHODS

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

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

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Receive data

Forwarding and receiving > Receive data

Showing 1-1 of 1 item

filter

New Receiving Port

Listen on this port	Status	Actions
9997	Enabled Disable	Delete

Searching in the splunk

Splunk Universal Forwarder - Splunk 8.1.2			
Search Results			
1 minute per column			
Format Timeline	Zoom Out	+ Zoom to Selection	X Deselect
	1	2	3
List	Format	20 Per Page	< Prev
<i>< Hide Fields</i>	<i>All Fields</i>	<i>i</i> Time Event	Next >
SELECTED FIELDS			
a host 1			
a source 2			
a sourcetype 2			
INTERESTING FIELDS			
# bytes 100+			
a clientip 2			
# date_hour 3			
# date_mday 1			
# date_minute 24			
a date_month 1			
# date_second 38			
a date_wday 1			
# date_year 1			
# date_zone 2			
a file 100+			
a ident 1			
a index 1			
# linecount 2			
a method 4			
a punct 49			
a referer 6			
a referrer_domain 1			
a req_time 54			
a root 2			

Finally the log of the hosted server is retrieved.

Summary

To host a website on an Ubuntu server and use Splunk to monitor login logs, you'll need to follow a few steps. Here's a general guide:

1. Set up your Ubuntu server: Install a web server like Apache or Nginx, and configure it to serve your website. Ensure that your website's access logs are enabled and accessible.
2. Install and configure Splunk: Install Splunk on your Ubuntu server by following the official installation instructions provided by Splunk. You can download the Splunk package appropriate for your Ubuntu version from the Splunk website.
3. Configure Splunk to monitor logs: Once Splunk is installed, you need to configure it to monitor the log files where login attempts are recorded. This could be the system logs (`/var/log/auth.log` or `/var/log/secure` on Ubuntu), or it could be custom logs generated by your web server.
 - Edit the Splunk inputs configuration file (`inputs.conf`) to specify which log files to monitor. You'll need to define a stanza for each log file you want Splunk to monitor.
 - For example, if you're monitoring Apache access logs, you would add a stanza like this:

```

```
[monitor:///var/log/apache2/access.log]
```

```
sourcetype = apache_access
```

```

- After making changes to `inputs.conf`, restart Splunk to apply the new configuration.

4. Search and analyse logs in Splunk: Once Splunk is configured to monitor the appropriate log files, you can use the Splunk web interface to search and analyse the logs. You can create custom searches and alerts to monitor for login events or any other specific activity you're interested in.

5. Set up dashboards and alerts: Splunk provides powerful visualisation tools that allow you to create dashboards to monitor and analyse your logs. You can create visualisations of login attempts over time, track failed login attempts, and set up alerts to notify you of suspicious activity.

6. Secure your system and Splunk instance: Make sure your Ubuntu server and Splunk instance are properly secured to prevent unauthorised access to your logs and sensitive data.

By following these steps, you'll be able to host your website on an Ubuntu server and use Splunk to monitor login logs and other activities on your server.