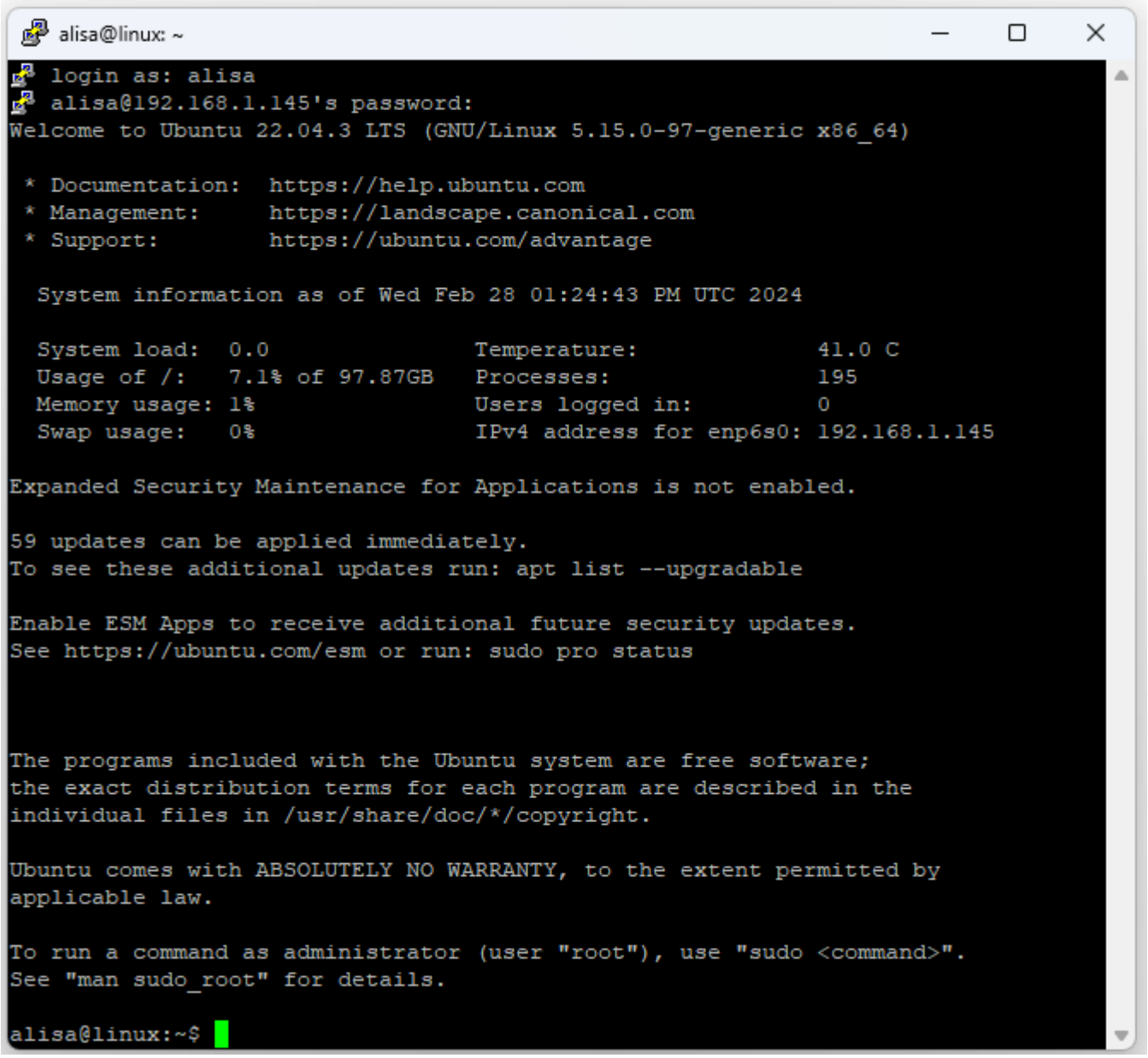
Установка Apache HTTP Server в Ubuntu 22.04

Введение

Apache HTTP Server является наиболее широко используемым веб-сервером в мире. Он предоставляет множество мощных функций, включая динамически загружаемые модули, надежную поддержку мультимедиа и обширную интеграцию с другим популярным программным обеспечением.

В этом руководстве мы проследим, как установить Apache HTTP Server на сервер Ubuntu 22.04.

Подключимся к нашему серверу через программу PuTTY, введем логин указанный при установке нашего сервера и пароль.



Предварительные условия

Прежде чем приступить к работе с этим руководством, на вашем сервере должен быть настроен обычный пользователь без полномочий root с привилегиями sudo. Кроме того, вам необходимо включить базовый брандмауэр для блокировки несущественных портов. Вы можете узнать, как настроить учетную запись обычного пользователя и настроить брандмауэр для вашего сервера, следуя нашему руководству по начальной настройке сервера для Ubuntu 20.04 .

Если у вас есть доступная учетная запись, для начала войдите в систему как пользователь без полномочий root.

Установка Apache

Apache доступен в репозиториях программного обеспечения Ubuntu по умолчанию, что позволяет установить его с помощью обычных инструментов управления пакетами.

Начнем с обновления локального индекса пакетов, чтобы отразить последние изменения исходного кода:

```
sudo apt update
```

Введем повторно пароль и дождемся окончания обновления индекса пакетов.

Установим непосредственно сам пакет Apache HTTP Server

```
sudo apt install apache2
```

```
alisa@linux:~$ sudo apt install apache2
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 bzip2 libaprl libaprutill
  libaprutill-dbd-sqlite3 libaprutill-ldap liblua5.3-0 mailcap mime-support
  ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
  bzip2-doc
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils bzip2 libaprl libaprutill
  libaprutill-dbd-sqlite3 libaprutill-ldap liblua5.3-0 mailcap mime-support
  ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 58 not upgraded.
Need to get 2,139 kB of archives.
After this operation, 8,518 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

После подтверждения установки apt install

```
Do you want to continue? [Y/n] **Y**
```

будет установлен Apache и все необходимые зависимости.

```
Progress: [ 70%] [#########################################.................]
```

Настройка брандмауэра

Перед тестированием Apache необходимо изменить настройки брандмауэра, чтобы разрешить внешний доступ к веб-портам по умолчанию. Предполагая, что вы следовали инструкциям, указанным в предварительных требованиях, у вас должен быть настроен брандмауэр UFW, ограничивающий доступ к вашему серверу.

Во время установки Apache регистрируется в UFW, чтобы предоставить несколько профилей приложений, которые можно использовать для включения или отключения доступа к Apache через брандмауэр.

Перечислите **ufw** профили приложений, набрав:

```
sudo ufw app list
```

```
alisa@linux:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  OpenSSH
alisa@linux:~$
```

Как видно из результатов, для Apache доступны три профиля:

- Apache : этот профиль открывает только порт 80 (обычный незашифрованный веб-

трафик).
- Apache Full : этот профиль открывает как порт 80 (обычный незашифрованный веб-трафик), так и порт 443 (зашифрованный трафик TLS/SSL).
- Apache Secure : этот профиль открывает только порт 443 (трафик с шифрованием TLS/SSL).

Рекомендуется включить наиболее ограничительный профиль, который по-прежнему будет разрешать настроенный вами трафик. Поскольку в этом руководстве мы еще не настроили SSL для нашего сервера, нам нужно будет разрешить трафик только через порт 80:

```
sudo ufw allow 'Apache'
```

```
alisa@linux:~$ sudo ufw allow 'Apache'
Rules updated
Rules updated (v6)
alisa@linux:~$
```

Правила обновлены и вы можете проверить изменение, набрав:

```
sudo ufw status
```

В результате, при включенном брандмауэре, будет предоставлен список разрешенного HTTP-трафика с уведомлением запись «Status: active» и мы смело переходим к главе **Проверка вашего веб-сервера**

```
alisa@linux:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Apache                     ALLOW       Anywhere
Apache (v6)                ALLOW       Anywhere (v6)

alisa@linux:~$
```

В случае же отключенного брандмауэра, мы получим запись «Status: inactive»

```
alisa@linux:~$ sudo ufw status
Status: inactive
```

Включение брандмауэра UFW в Ubuntu

Как только мы обнаружим, что брандмауэр не активен, проверим, добавлены ли к нему какие-либо правила. Эта команда будет работать, даже если брандмауэр неактивен.

```
sudo ufw show added
```

```
alisa@linux:~$ sudo ufw status
Status: inactive
alisa@linux:~$ sudo ufw show added
Added user rules (see 'ufw status' for running firewall):
ufw allow Apache
```

Проверим правила и убедимся, что если мы включим брандмауэр, с нашим сервером все будет в порядке. А затем включим брандмауэр с подтверждением наших действий клавишей **Y**.

```
sudo ufw enable
```

```
alisa@linux:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Снова проверим статус брандмауэра UFW ранее использованной командой:

```
sudo ufw status
```

```
alisa@linux:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Apache                     ALLOW       Anywhere
Apache (v6)                ALLOW       Anywhere (v6)

alisa@linux:~$
```

Брандмауэр успешно активирован.

Проверка вашего веб-сервера

Наш веб-сервер уже должен быть установлен и запущен. Проверим **systemd** систему инициализации, чтобы убедиться, что служба работает, набрав:

```
sudo systemctl status apache2
```

```
alisa@linux:~$ sudo systemctl status apache2
[sudo] password for alisa:
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
     Active: active (running) since Wed 2024-02-28 13:40:18 UTC; 54min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2751 (apache2)
      Tasks: 55 (limit: 19032)
     Memory: 5.5M
        CPU: 204ms
     CGroup: /system.slice/apache2.service
             ├─2751 /usr/sbin/apache2 -k start
             ├─2752 /usr/sbin/apache2 -k start
             └─2753 /usr/sbin/apache2 -k start

Feb 28 13:40:18 linux systemd[1]: Starting The Apache HTTP Server...
Feb 28 13:40:18 linux apachectl[2750]: AH00558: apache2: Could not reliably det>
Feb 28 13:40:18 linux systemd[1]: Started The Apache HTTP Server.
```

From:
https://wwoss.ru/ - **worldwide open-source software**

Permanent link:
https://wwoss.ru/doku.php?id=software:linux_server:ubuntu_server_install_apache&rev=1709131083

Last update: **2024/02/28 17:38**