

在 Ubuntu 16.04 上安裝 vsftpd

ref: <https://askubuntu.com/questions/575523/how-to-setup-virtual-users-for-vsftpd-with-access-to-a-specific-sub-directory>

目前的開發環境為資料庫伺服器主機、網站伺服器主機和開發系統用電腦分別為不同的實體電腦，而且資料庫伺服器主機和網站伺服器主機均為 Ubuntu 16.04 作業系統，而開發用電腦為 Windows 7 作業系統。同時，網站伺服器主機使用 Apache HTTP Server 軟體來提供網站服務。因此，如何將在開發系統電腦上完成的系統上傳到網站伺服器主機，就是一個需要思考的問題。在此，我提出在網站伺服器主機安裝 vsftpd 伺服器端軟體及在開發系統端安裝 FileZilla 軟體，將完成的系統透過 FTP 協定將網站上傳的方法。執行程序如下：

我的目的是在網站伺服器主機上建立一個虛擬用戶，例如 apache 帳號，並限制只能存取 /var/www 目錄下的特定子目錄，例如 /var/www/apache 子目錄，使用虛擬用戶的目的是防止被利用此帳號登入 Ubuntu 系統，以維護網站伺服器主機的安全性。

1. 安裝 vsftpd 軟體

```
$ sudo apt-get install vsftpd libpam-pwdfile
```

2. 編輯 /etc/vsftpd.conf

為了預防失敗，先備份 /etc/vsftpd.conf，再修改內容。

```
$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
```

```
$ sudo nano /etc/vsftpd.conf
```

修改後的 /etc/vsftpd.conf 內容：

```
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
```

```
local_root=/var/www
chroot_local_user=YES
allow_writeable_chroot=YES
hide_ids=YES

#virtual user settings
user_config_dir=/etc/vsftpd_user_conf
guest_enable=YES
virtual_use_local_privs=YES
pam_service_name=vsftpd
nopriv_user=vsftpd
guest_username=vsftpd
```

3. 建立用戶帳號：

You can either use a database or `htpasswd`, I found `htpasswd` faster and easier to use.
make a directory to store your users

在此，範例使用的帳號名稱為 apache

```
$ sudo mkdir /etc/vsftpd
$ sudo htpasswd -cd /etc/vsftpd/ftpd.passwd apache
```

adding additional users just omit the `-c`

(如果需要建立第二個 (含) 以後的帳號不需要 `-c` 參數)

```
$ sudo htpasswd -d /etc/vsftpd/ftpd.passwd laravel
```

Once your users are created you can now change your PAM config file

```
$ sudo cp /etc/pam.d/vsftpd /etc/pam.d/vsftpd.bak
$ sudo nano /etc/pam.d/vsftpd
```

在此，我先將 `/etc/pam.d/vsftpd` 備份為 `/etc/pam.d/vsftpd.bak` 再進行編輯。

and remove everything inside this file and replace with the following

```
auth      required      pam_pwdfile.so pwdfile /etc/vsftpd/ftpd.passwd
```

```
account    required    pam_permit.so
```

This will enable login for your virtual users defined in `/etc/vsftpd/ftpd.passwd` and will disable local users

Next we need to add a user for these virtual users to use. These users will not have access to the shell and will be called `vsftpd`

```
$ sudo useradd --home /home/vsftpd --gid nogroup -m --shell /bin/false vsftpd
```

the user must match `guest_username=vsftpd` in the vsftpd conf file

4. Defining Directory Access

在此節，我們必須為每一個虛擬用戶建立各別的目錄存取權限組態設定檔，稱為 `vsftpd` 用戶組態設定 (`vsftpd_user_conf`)，裡面說明了可以存取的目錄路徑和權限。而這些 `vsftpd_user_conf` 的儲存路徑和 `/etc/vsftpd.conf` 檔案中的 `user_config_dir` 參數指定的位置有關，所以我們回去查看 `/etc/vsftpd.conf`，發現設定如下：

```
$ user_config_dir=/etc/vsftpd_user_conf
```

因此，`apache` 帳號的 `vsftpd` 用戶組態設定應該是 `/etc/vsftpd_user_conf/apache`。

由於範例的目的是將 `apache` 用戶的路徑瀏覽權限限制於 `/var/www/apache`，且不得向上層目錄瀏覽，因此必須將 `apache` 帳號的 `ftp` 根目錄設定於 `/etc/vsftpd_user_conf/apache` 中。執行程序如下：

```
$ sudo mkdir /etc/vsftpd_user_conf
$ sudo nano /etc/vsftpd_user_conf/apache
```

在 `/etc/vsftpd_user_conf/apache` 中加入以下內容：

```
local_root=/var/www/apache
```

所以同時，我們必須建立 `/var/www/apache` 目錄。

```
$ sudo mkdir /var/www/apache
```

由於使用 `sudo` 指令建立的目錄，其存取權限是屬於 `root` 帳號和群組的，所以需要改變 `/var/www/apache` 目錄的存取權限。

在此，我的目的是讓 `apache` 帳號在 `/var/www/apache` 目錄，也就是登入的根目錄，沒有寫入權限，僅有讀取及執行權限，並開放一個 `www` 子目錄提供完整的寫入、讀取和執行權限。因此，執行程序如下：

```
$ sudo chmod -w /var/www/apache
$ sudo mkdir /var/www/apache/www
$ sudo chmod -R 755 /var/www/apache/www
$ sudo chown -R vsftpd:nogroup /var/www/apache
```

然後，重啟 `vsftpd` 服務。

```
$ sudo service vsftpd restart
```

5. 在本地端使用終端機執行 `ftp` 連線測試:

打開終端機，輸入 `ftp [IP address]`，並輸入帳號和密碼後，如果可以登入就是成功了。

執行程序如下：

```
user@Morpheus:~$ ftp 127.0.0.1
Connected to 10.10.1.104.
220 (vsFTPd 3.0.3)
Name (10.10.1.104:user): apache
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

6. 在遠地端使用 `FileZilla` 執行連線測試：

在開發用電腦中安裝 `FileZilla Client` 軟體，並嘗試執行 `FTP` 連線時，則出現 "無法取得目錄列表" 的訊息，這是因為 `FileZilla Client` 的預設傳輸模式為「被動模式」，將其改為

「主動模式」就好了。其位置在『編輯 -> 設定 -> 連線 -> FTP -> 傳輸模式』，點選「主動模式」再按「確認」就好了。

2017.05.04 by Morpheus