**THAO TÁC THỰC HIỆN CẤU HÌNH FTP SERVER**

# **CẤU HÌNH DNS - TẢI GÓI BIND**

Để thực hiện cấu hình FTP Server, trước hết, trên máy chúng ta cần phải cấu hình DNS.

Để cấu hình được DNS Server, ta cần gói BIND

Do kho repo chứa thư viện liên quan đến BIND đã bị đổi sang **vault.centos.org** nên ta cần phải cấu hình lại đường dẫn tải thư viện:

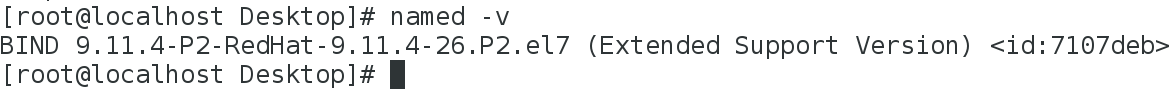
* B1: gõ lệnh “**gedit /etc/yum.repos.d/CentOS-Base.repo**” để vào cấu hình file.
* B2: Tìm tất cả các dòng bắt đầu bằng “**mirrorlist=”** và thêm dấu **#** trước chúng để vô hiệu hóa. Sau đó, tìm dòng bắt đầu bằng “**baseurl=”** và cập nhật lại như sau:

**baseurl=**[**http://vault.centos.org/7.9.2009/os/$basearch/**](http://vault.centos.org/7.9.2009/os/$basearch/)

**hoặc bạn có thể copy nội dung bên dưới để dán vào file CentOS-Base.repo**

| # CentOS-Base.repo  #  # The mirror system uses the connecting IP address of the client and the  # update status of each mirror to pick mirrors that are updated to and  # geographically close to the client. You should use this for CentOS updates  # unless you are manually picking other mirrors.  #  # If the mirrorlist= does not work for you, as a fall back you can try the  # remarked out baseurl= line instead.  #  #  [base]  name=CentOS-$releasever - Base  #mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra  baseurl=http://vault.centos.org/centos/$releasever/os/$basearch/  gpgcheck=1  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7  #released updates  [updates]  name=CentOS-$releasever - Updates  #mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$infra  baseurl=http://vault.centos.org/centos/$releasever/updates/$basearch/  gpgcheck=1  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7  #additional packages that may be useful  [extras]  name=CentOS-$releasever - Extras  #mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infra  baseurl=http://vault.centos.org/centos/$releasever/extras/$basearch/  gpgcheck=1  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7  #additional packages that extend functionality of existing packages  [centosplus]  name=CentOS-$releasever - Plus  #mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=centosplus&infra=$infra  baseurl=http://vault.centos.org/centos/$releasever/centosplus/$basearch/  gpgcheck=1  enabled=0  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7 |
| --- |

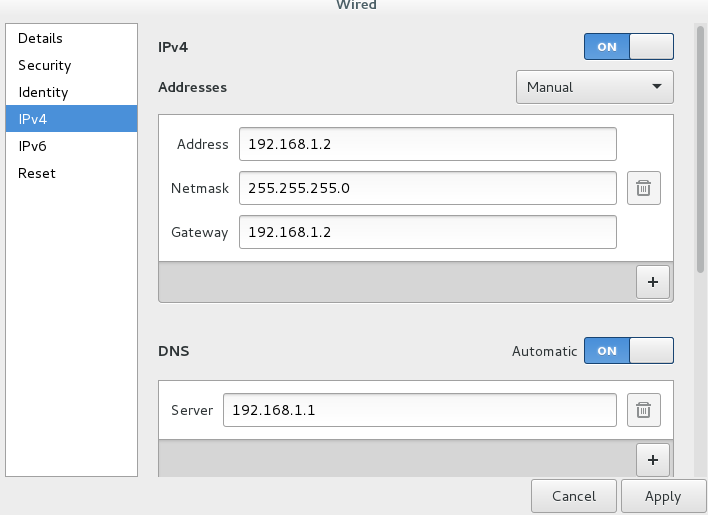
* B3: Sau khi sửa xong, lưu file lại và tiến hành tải gói **BIND** về bằng lệnh “**yum install bind bind-utils –y**” (lưu ý: cần kiểm tra kết nối mạng trước khi tải bằng lệnh ping 8.8.8.8)
* B4: Sau khi tải xong, tiến hành kiểm tra xem **BIND** đã có trên máy chưa bằng lệnh “**named -v**”

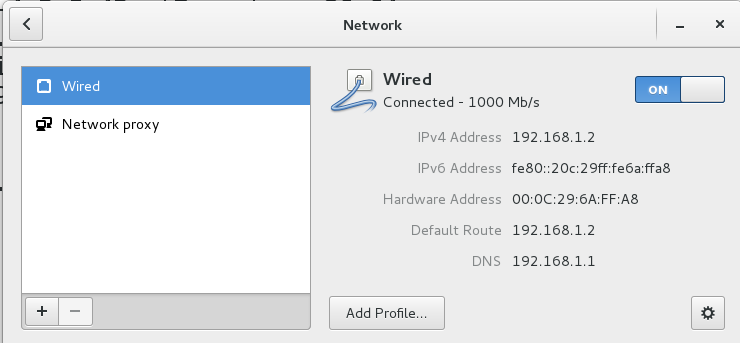


# 

# **CÁC BƯỚC CẤU HÌNH DNS**

**B1**: Cần thiết lập **ip tĩnh** trước khi tiến hành cấu hình DNS.





**B2**: Sau khi thiết lập IP tĩnh xong. Tiến hành bắt đầu cấu hình DNS. Đầu tiên vào file **named.conf** và cấu hình bằng lệnh

* **gedit /etc/named.conf**

Sau đó tiến hành thay đổi một số thông tin bên trong tệp **named.conf** như sau:





Sau khi thay đổi xong, tiến hành lưu file **named.conf** lại.

**B3**: Tiến hành truy cập file **named.rfc1912.zone** để thêm phân giải xuôi (Forward) và phân giải ngược (Reverse) bằng câu lệnh:

* **gedit /etc/named.rfc1912.zones**

Sau khi mở được file, tiến hành thêm phần phân giải xuôi và phân giải ngược vào bên dưới cùng của file:

| zone "sgu.edu.vn" IN {  type master;  file "forward.sgu.edu.vn";  allow-update { none; };  };  zone "1.168.192.in-addr.arpa" IN {  type master;  file "reverse.192.168.1.0";  allow-update { none; };  }; |
| --- |

Sau khi thêm xong, lưu file lại và đóng file.

**B4**: Sau khi đã khai báo xong các phần zone thuận và zone nghịch, ta khai báo các file lưu trữ record của các file này.

Vào file lưu trữ record của phân giải xuôi bằng lệnh:

* **gedit /var/named/forward.sgu.edu.vn**

Lúc này tệp **forward.sgu.edu.vn** sẽ là tệp trống. Bắt đầu tạo bản record bằng cách thêm nội dung sau vào tệp:

| $TTL 86400  @ IN SOA server.sgu.edu.vn. root.sgu.edu.vn. (  2018210902 ;Serial (nên tăng số này lên)  3600 ;Refresh  1800 ;Retry  604800 ;Expire  86400 ;Minimum TTL  )  @ IN NS server.sgu.edu.vn.  @ IN A 192.168.1.2  server IN A 192.168.1.2 ; Thêm bản ghi A cho name server  www IN A 192.168.1.2 ; Nếu cần subdomain www |
| --- |

Resource record A chỉ việc phân giải domain sgu.edu.vn sẽ trỏ về IP 192.168.1.2

Sau khi thêm xong tiến hành lưu file lại.

Vào file lưu trữ record của phân giải ngược bằng lệnh:

* **gedit /var/named/reverse.192.168.1.0**

Lúc này tệp **reverse.192.168.1.0** sẽ là tệp trống. Bắt đầu tạo bản record bằng cách thêm nội dung sau vào tệp:

| $TTl 86400  @ IN SOA server.sgu.edu.vn. root.sgu.edu.vn. (  2011071001 ;Serial  3600 ;Refresh  1800 ;Retry  604800 ;Expire  86400 ;Minimum TTL  )  @ IN NS server.sgu.edu.vn.  2 IN PTR server.sgu.edu.vn.  2 IN PTR sgu.edu.vn. |
| --- |

Resource record PTR chỉ địa chỉ tương ứng sẽ trỏ về domain nào. Trong tình huống này, 2 có nghĩa là 192.168.1.2 (kết hợp với lớp mạng 192.168.1.0), sẽ trỏ về domain: **sgu.edu.vn.** và **server.sgu.edu.vn.**

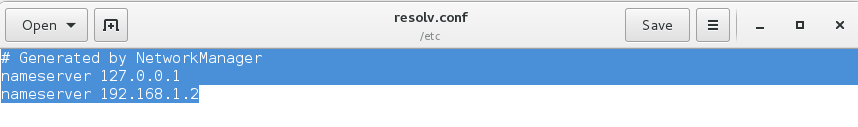
Tiến hành lưu và đóng file lại.

**B4**: kiểm tra file **/etc/resolv.conf** xem có cấu hình nameserver đúng chưa.

* **gedit /etc/resolv.conf**

Trong file phải có dòng: **nameserver 127.0.0.1**

Do bạn đang chạy DNS server local.



**B5**: Khởi động DNS bằng lệnh sau:

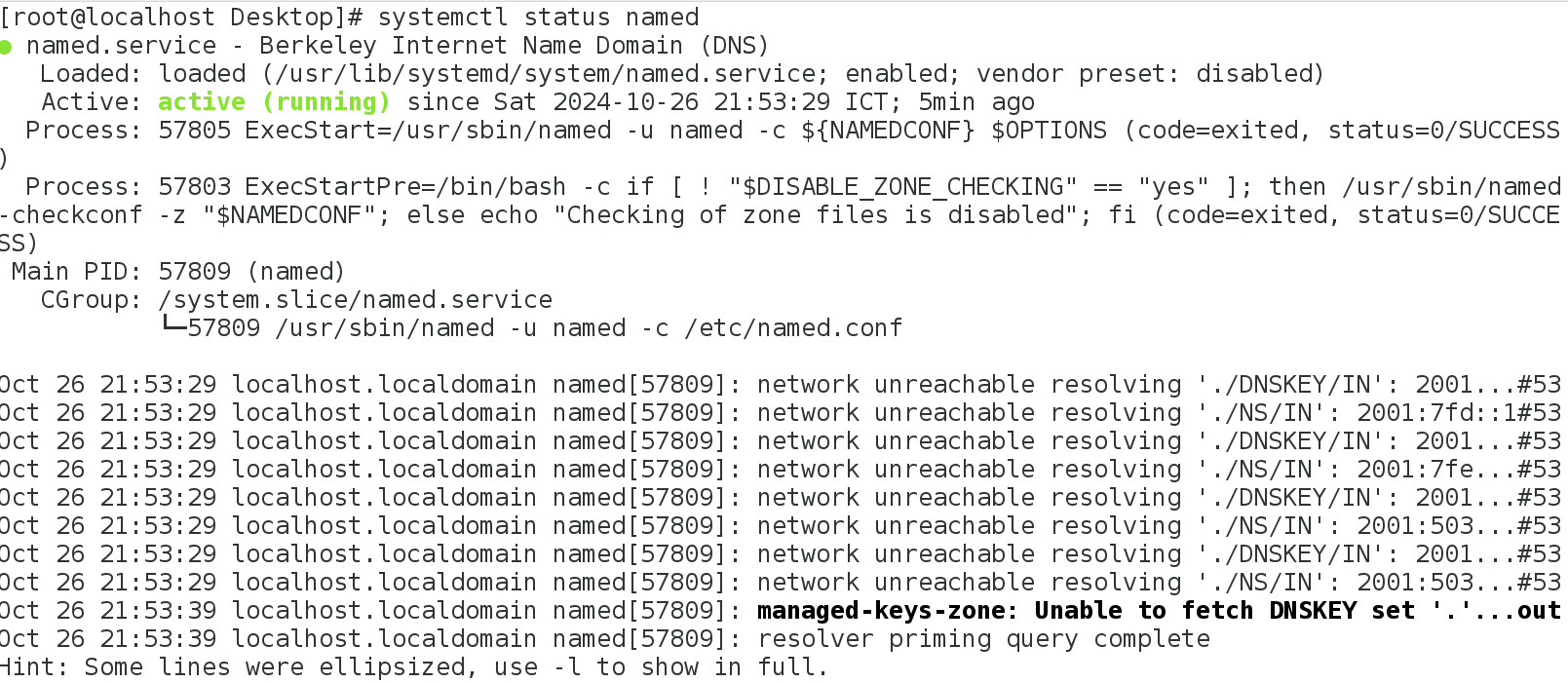
* **systemctl enable named**
* **systemctl start named**

**Lưu ý**: bạn cần phải loại bỏ tường lửa bằng lệnh sau để tránh gặp lỗi:

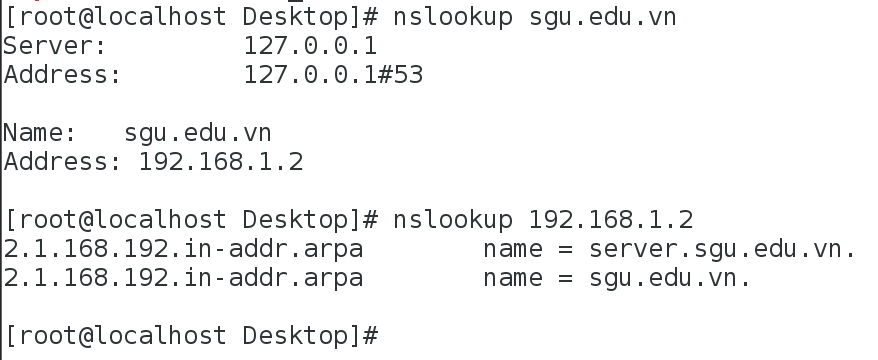
* **yum remove firewalld -y**

**B6**: tiến hành kiểm tra trạng thái của DNS bằng lệnh:

* **systemctl status named**



**B7**: thực hiện lệnh **nslookup** để kiểm tra.



# 

# **TẢI THƯ VIỆN VSFTPD**

**Công dụng:**

vsftpd (Very Secure FTP Daemon) là một dịch vụ FTP (File Transfer Protocol) trên CentOS và các hệ điều hành Linux khác. Nó được thiết kế để cung cấp một phương thức truyền tải tệp tin qua mạng một cách an toàn, nhanh chóng và dễ quản lý.

**Các mục đích chính của vsftpd trên CentOS:**

1. **Cung cấp dịch vụ truyền tải tệp tin (FTP server)**:
   * vsftpd cho phép người dùng tải lên hoặc tải xuống tệp tin giữa máy chủ và các máy khách, thuận tiện cho việc chia sẻ và sao lưu dữ liệu trong hệ thống mạng nội bộ hoặc qua Internet.
2. **Thiết lập các quyền và chính sách bảo mật**:
   * vsftpd cung cấp nhiều tùy chọn bảo mật như:
     + **Người dùng ẩn danh** (Anonymous User): cho phép tải xuống tệp tin công khai.
     + **Người dùng hệ thống và người dùng ảo**: kiểm soát người dùng cụ thể có quyền truy cập.
     + **Chroot Jail**: giới hạn quyền truy cập của người dùng vào thư mục riêng của họ, ngăn không cho họ truy cập các phần khác của hệ thống.
     + **TLS/SSL**: mã hóa dữ liệu truyền tải qua mạng, giúp bảo vệ thông tin đăng nhập và tệp tin tránh khỏi các cuộc tấn công.
3. **Quản lý truyền tải tệp tin cho các dịch vụ khác**:
   * vsftpd thường được sử dụng trong các dịch vụ như web server, ứng dụng chia sẻ dữ liệu nội bộ và nhiều ứng dụng khác, cho phép quản trị viên quản lý việc truyền tải các tệp cấu hình, bản cập nhật, sao lưu và các loại dữ liệu khác một cách an toàn.
4. **Tính ổn định và hiệu suất cao**:
   * vsftpd được thiết kế để xử lý một lượng lớn người dùng và yêu cầu truyền tải cùng lúc mà vẫn duy trì hiệu suất và độ ổn định cao, phù hợp cho các hệ thống lớn và các server hoạt động 24/7.

Với những tính năng này, vsftpd là một trong các công cụ FTP server phổ biến cho các hệ thống Linux như CentOS, được sử dụng để triển khai các dịch vụ FTP an toàn, nhanh chóng và quản lý người dùng dễ dàng.

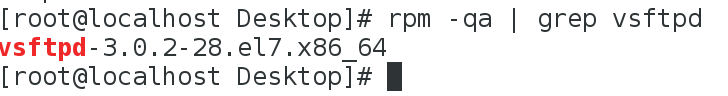
**Các bước thực hiện**:

Do kho repo chứa thư viện liên quan đến vsftpd đã bị đổi sang **vault.centos.org** nên ta cần phải cấu hình lại đường dẫn tải thư viện:

* B1: gõ lệnh “**gedit /etc/yum.repos.d/CentOS-Base.repo**” để vào cấu hình file.
* B2: Tìm tất cả các dòng bắt đầu bằng “**mirrorlist=”** và thêm dấu **#** trước chúng để vô hiệu hóa. Sau đó, tìm dòng bắt đầu bằng “**baseurl=”** và cập nhật lại như sau:

**baseurl=http://vault.centos.org/7.9.2009/os/$basearch/**

* B3: sau khi sửa xong, lưu file lại và tiến hành tải thư viện **vsftpd** về bằng lệnh “**yum install vsftpd -y**” (lưu ý: cần kiểm tra kết nối mạng trước khi tải bằng lệnh ping 8.8.8.8)
* B4: Sau khi tải xong, tiến hành kiểm tra xem có thư viện **vsftpd** xem đã có trên máy chưa bằng lệnh
  + **rpm -qa | grep vsftpd**



| [base]  name=CentOS-$releasever - Base  baseurl=http://vault.centos.org/7.9.2009/os/$basearch/  gpgcheck=1  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7  [updates]  name=CentOS-$releasever - Updates  baseurl=http://vault.centos.org/7.9.2009/updates/$basearch/  gpgcheck=1  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7  [extras]  name=CentOS-$releasever - Extras  baseurl=http://vault.centos.org/7.9.2009/extras/$basearch/  gpgcheck=1  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7  [centosplus]  name=CentOS-$releasever - Plus  baseurl=http://vault.centos.org/7.9.2009/centosplus/$basearch/  gpgcheck=1  enabled=0  gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7 |
| --- |

# 

# **TẢI THƯ VIỆN FTP**

**Công dụng:**

Trên CentOS, gói ftp chủ yếu được sử dụng để cung cấp khả năng **truyền tải tệp tin** giữa máy khách và máy chủ thông qua giao thức FTP (File Transfer Protocol). FTP là một giao thức mạng tiêu chuẩn cho phép truyền tải tệp tin một cách dễ dàng và nhanh chóng trong hệ thống mạng, dù là mạng nội bộ hay qua Internet.

**Các mục đích chính của gói ftp trên CentOS:**

1. **Kết nối đến FTP Server để tải lên và tải xuống tệp tin**:
   * Gói ftp trên CentOS cung cấp các công cụ dòng lệnh cho phép người dùng kết nối đến các máy chủ FTP để thực hiện các thao tác tải tệp lên (upload) hoặc tải tệp xuống (download).
2. **Chia sẻ dữ liệu giữa các hệ thống**:
   * FTP được sử dụng rộng rãi trong việc chia sẻ dữ liệu giữa các hệ thống Linux và cả với các hệ điều hành khác như Windows. Điều này hữu ích trong môi trường công ty hoặc mạng lưới, nơi các máy chủ lưu trữ tệp có thể dễ dàng chia sẻ tài nguyên cho nhiều người dùng.
3. **Tương tác và quản lý máy chủ từ xa**:
   * Gói ftp cũng cho phép quản trị viên hệ thống có thể đăng nhập và quản lý tệp tin trên các máy chủ từ xa một cách dễ dàng. Ngoài ra, họ cũng có thể sử dụng các lệnh như put, get, ls, cd để thực hiện các tác vụ cơ bản trên thư mục và tệp.
4. **Phục vụ việc sao lưu dữ liệu**:
   * FTP thường được sử dụng cho các tác vụ sao lưu dữ liệu từ xa. Các hệ thống sao lưu tự động có thể dùng ftp để sao lưu các tệp tin lên các máy chủ từ xa hoặc các dịch vụ đám mây hỗ trợ giao thức FTP.
5. **Triển khai và cập nhật ứng dụng**:
   * Nhiều ứng dụng có thể được triển khai hoặc cập nhật từ xa thông qua FTP, giúp cho các lập trình viên hoặc quản trị viên hệ thống dễ dàng quản lý mã nguồn và phiên bản của ứng dụng trực tiếp trên các máy chủ.

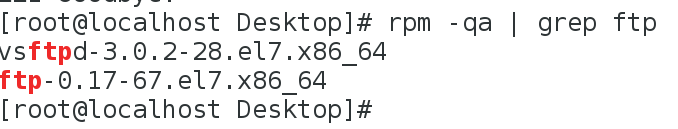
**Các bước thực hiện**:

Do kho repo chứa thư viện liên quan đến vsftpd đã bị đổi sang **vault.centos.org** nên ta cần phải cấu hình lại đường dẫn tải thư viện:

* B1: gõ lệnh “**gedit /etc/yum.repos.d/CentOS-Base.repo**” để vào cấu hình file.
* B2: Tìm tất cả các dòng bắt đầu bằng “**mirrorlist=”** và thêm dấu **#** trước chúng để vô hiệu hóa. Sau đó, tìm dòng bắt đầu bằng “**baseurl=”** và cập nhật lại như sau:

**baseurl=http://vault.centos.org/7.9.2009/os/$basearch/**

* B3: sau khi sửa xong, lưu file lại và tiến hành tải thư viện **vsftpd** về bằng lệnh “**yum install ftp -y**” (lưu ý: cần kiểm tra kết nối mạng trước khi tải bằng lệnh ping 8.8.8.8)
* B4: Sau khi tải xong, tiến hành kiểm tra xem có thư viện **ftp** xem đã có trên máy chưa bằng lệnh
  + **rpm -qa | grep ftp**



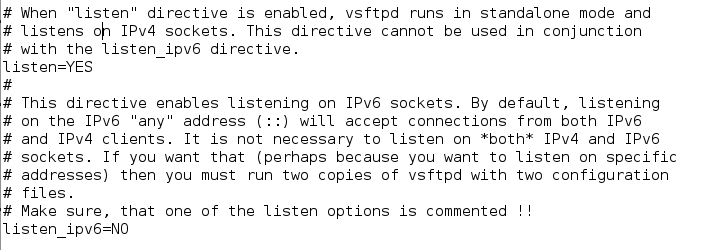
# 

# **KHỞI CHẠY FTP BAN ĐẦU**

Sau khi đã tải 2 thư viện ftp và vsftpd, ta có thể khởi chạy ftp mặc định bằng các thao tác sau:

**B1:** ta cần vào thư mục vsftpd.conf để kiểm tra xem đã thiết lập IPv4 và IPv6 chưa

* **gedit /etc/vsftpd/vsftpd.conf**

****

Cấu hình giá trị ngay chỗ “**listen = Yes**” và “**listen\_ipv6 = No**”.

**Đây là file vsftpd.conf mặc định**

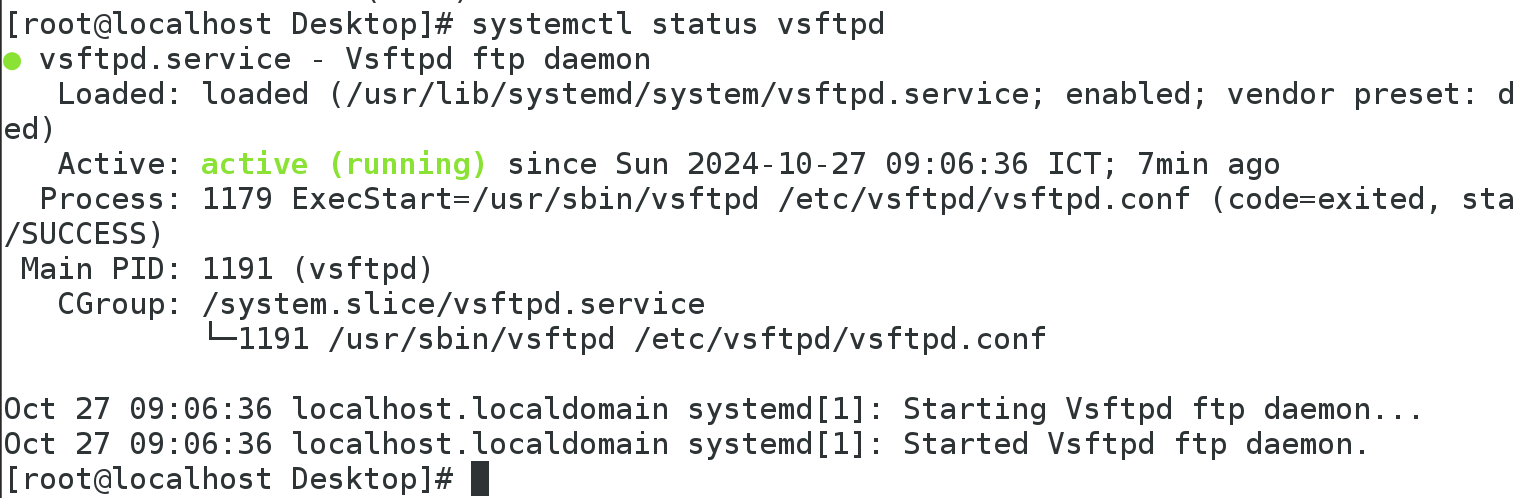
| **anonymous\_enable=YES**  **local\_enable=YES**  **write\_enable=YES**  **local\_umask=022**  **dirmessage\_enable=YES**  **xferlog\_enable=YES**  **connect\_from\_port\_20=YES**  **xferlog\_std\_format=YES**  **listen=NO**  **listen\_ipv6=YES**  **pam\_service\_name=vsftpd**  **userlist\_enable=YES**  **tcp\_wrappers=YES** |
| --- |

**B2**: Bắt đầu khởi chạy ftp bằng lệnh:

* **systemctl start vsftpd**
* **systemctl enable vsftpd**

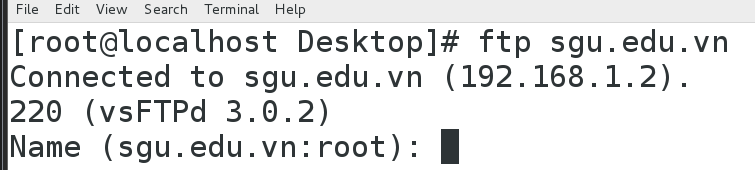
**B3**: kiểm tra trạng thái:

* **systemctl status vsftpd**

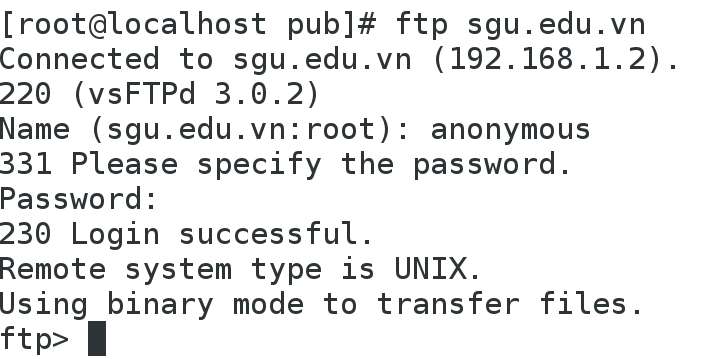


**B4**: Thử kết nối đến miền đã cấu hình bên phần cấu hình DNS:

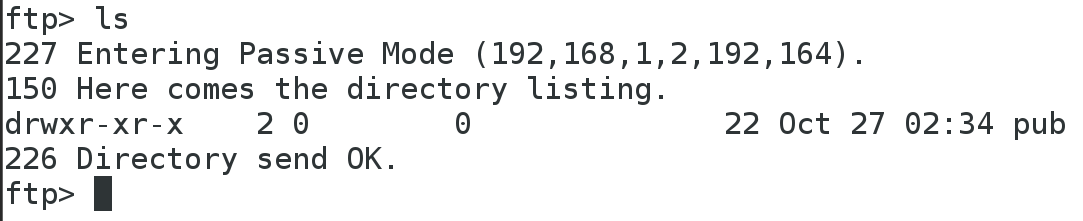
* **ftp sgu.edu.vn**



Tại đây, bạn có thể đăng nhập với name mặc định là **anonymous** và mật khẩu là **mật khẩu thiết lập lúc đăng nhập vào centOS trên máy các bạn**.

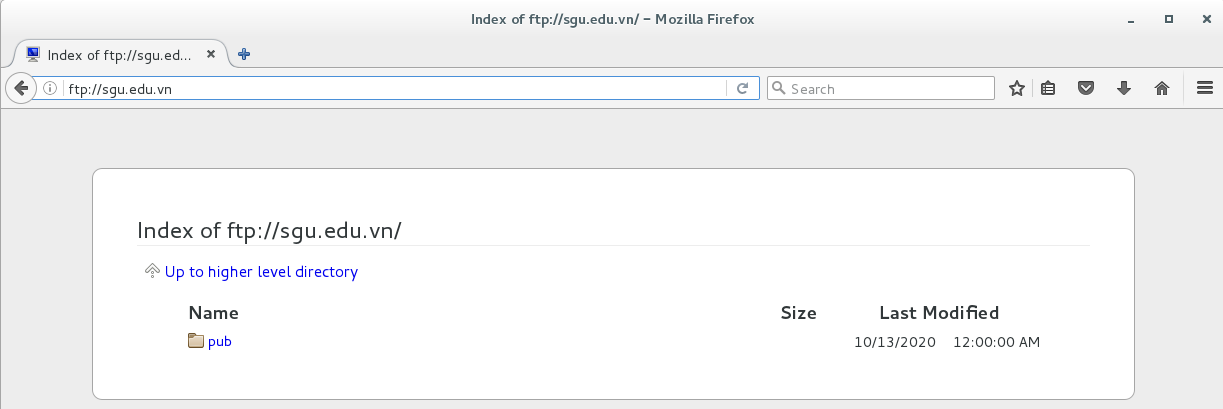


Và bạn có thể kiểm tra xem có thư mục nào trong ftp bằng lệnh **ls**



Như bạn thấy, nó thông báo đang có một thư mục gốc tên là **pub** trong ftp.

Hoặc bạn có thể truy cập trình duyệt Mozilla FireFox trên CentOS 7 và nhập đường dẫn “**ftp://sgu.edu.vn**”.



Nếu thực hiện được kết quả ở bước 3 có nghĩa là khởi động thành công ftp.

Còn nếu không hãy kiểm tra lại phần cấu hình DNS xem đã thành công hay chưa. (xem lại phần kết quả cuối cùng cấu hình DNS khi thực hiện lệnh **nslookup**)

**B5**: Ban đầu thư mục **pub** là thư mục rỗng. Tiến hành tạo một file trong thư mục **pub** trên máy và kiểm tra lại.

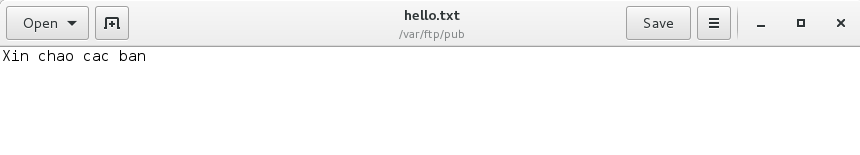
Di chuyển vào thư mục **pub** của ftp:

* **cd /var/ftp/pub**



Tiến hành tạo một file **hello.txt** với nội dung tùy chỉnh:

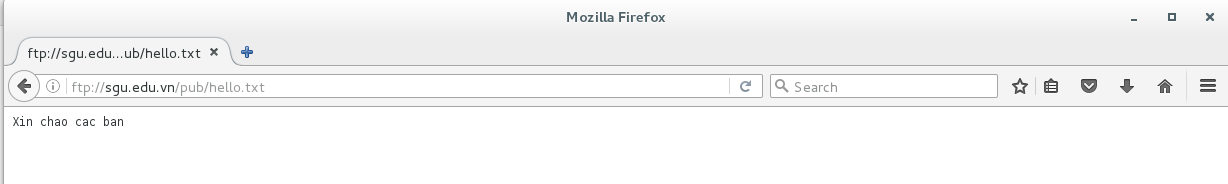
* **gedit hello.txt**



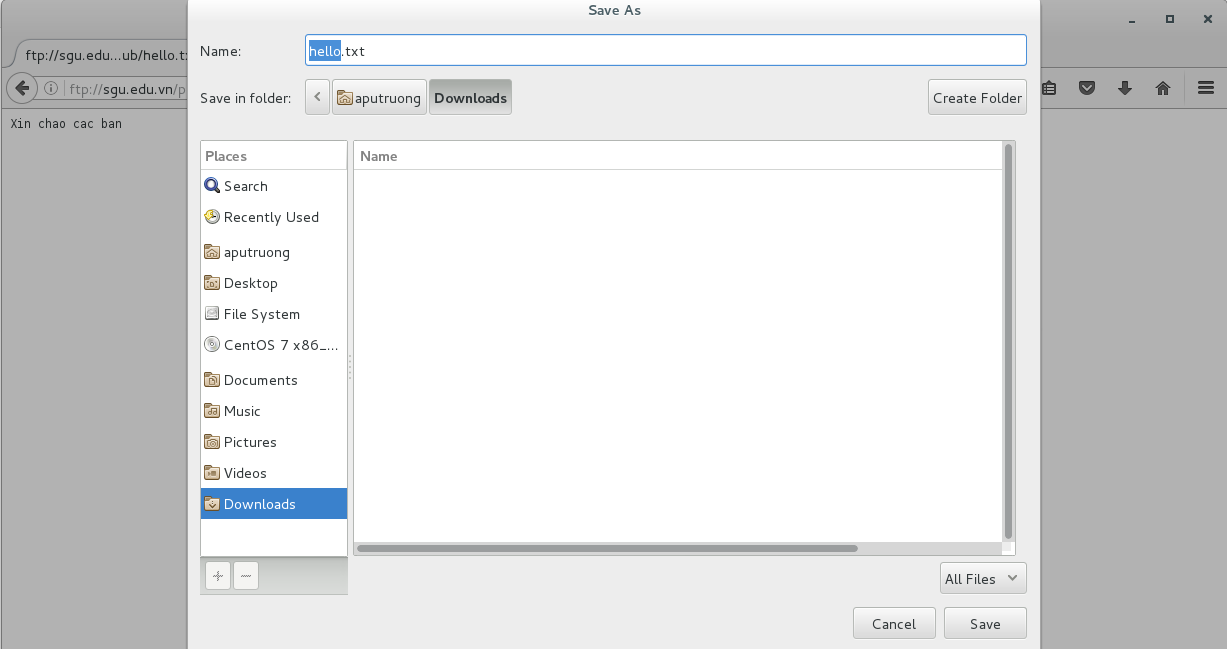
Giờ ta vào Mozilla FireFox để kiểm tra lại bằng cách nhập đường dẫn “**ftp://sgu.edu.vn**” và click vào thư mục **pub**. Ta sẽ thấy file **hello.txt** mà ta vừa tạo trên máy.

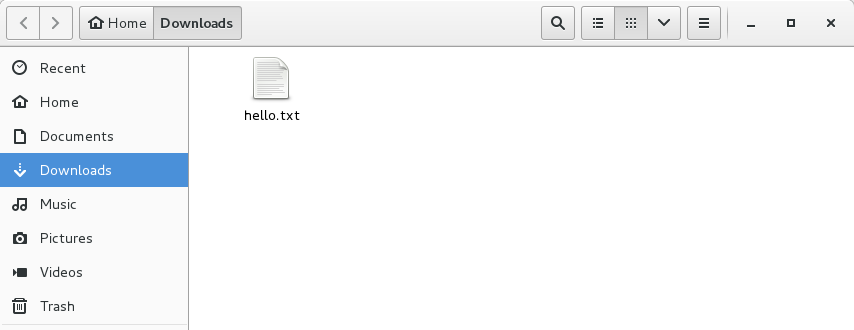


Ấn vào file **hello.txt**, ta có thể thấy thông điệp có trong file:



Và ta có thể tải file đó ngược lại về máy bằng các click chuột phải chọn **“Save Page As”** và chọn mục cần lưu file tải xuống:





# 

# **KHỞI CHẠY FTP VỚI USER**

Do mặc định ban đầu, ftp khởi chạy với **user anonymous.** Giờ ta muốn **ftp ngắt user anonymous** và sử dụng các user do ta thiết lập thì thực hiện các bước như sau:

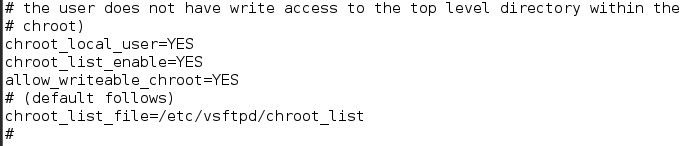
**B1**: Thiết lập cấu hình trong file **vsftpd.conf**

* **gedit /etc/vsftpd/vsftpd.conf**

Sau khi truy cập được vào file, tiến hành cấu hình lại như bên dưới:



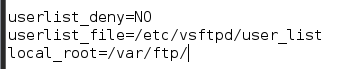








Thêm các nội dung bên dưới ở cuối file:



Hoặc copy nội dung này paste vào file **vsftpd.conf**

| **anonymous\_enable=NO**  local\_enable=YES  write\_enable=YES  local\_umask=022  dirmessage\_enable=YES  xferlog\_enable=YES  connect\_from\_port\_20=YES  xferlog\_std\_format=YES  **chroot\_local\_user=YES**  **chroot\_list\_enable=YES**  **allow\_writeable\_chroot=YES**  **chroot\_list\_file=/etc/vsftpd/chroot\_list**  **listen=YES**  **listen\_ipv6=NO**  pam\_service\_name=vsftpd  userlist\_enable=YES  tcp\_wrappers=YES  **userlist\_deny=NO**  **userlist\_file=/etc/vsftpd/user\_list**  **local\_root=/var/ftp/** |
| --- |

**anonymous\_enable=NO**:

* Không cho phép người dùng ẩn danh (anonymous) đăng nhập vào máy chủ FTP. Điều này làm tăng tính bảo mật bằng cách yêu cầu tất cả người dùng phải có tài khoản hợp lệ.

**local\_enable=YES**:

* Cho phép người dùng địa phương (local users) đăng nhập vào máy chủ FTP. Những người dùng này phải có tài khoản trên hệ thống.

**write\_enable=YES**:

* Cho phép người dùng thực hiện các thao tác ghi, như tải lên, xoá và thay đổi tệp tin trên máy chủ FTP. Nếu NO, tất cả các thao tác ghi sẽ bị chặn.

**local\_umask=022**:

* Đặt umask mặc định cho người dùng địa phương khi họ tải lên tệp. 022 sẽ thiết lập quyền mặc định cho tệp là 755, tức là chủ sở hữu có tất cả quyền, trong khi nhóm và người khác chỉ có quyền đọc và thực thi.

**dirmessage\_enable=YES**:

* Hiển thị thông báo thư mục khi người dùng vào một thư mục cụ thể. Thông báo này có thể được thiết lập trong tệp .message trong thư mục đó.

**xferlog\_enable=YES**:

* Kích hoạt ghi lại nhật ký các thao tác truyền tải tệp (như tải lên và tải xuống). Tất cả hoạt động sẽ được ghi vào tệp xferlog.

**connect\_from\_port\_20=YES**:

* Đảm bảo rằng kết nối dữ liệu (data connection) sẽ sử dụng cổng 20, một yêu cầu tiêu chuẩn của FTP.

**xferlog\_std\_format=YES**:

* Định dạng nhật ký theo chuẩn xferlog để dễ dàng phân tích và tương thích với các công cụ xử lý nhật ký FTP.

**chroot\_local\_user=YES**:

* Chroot người dùng vào thư mục cá nhân của họ, ngăn không cho họ truy cập vào các thư mục hệ thống bên ngoài. Điều này tạo một lớp bảo mật bổ sung.

**chroot\_list\_enable=YES**:

* Kích hoạt danh sách chroot\_list\_file, nơi bạn có thể chỉ định người dùng ngoại lệ không bị giới hạn bởi chroot.

**allow\_writeable\_chroot=YES**:

* Cho phép các thư mục gốc (chroot) có quyền ghi, điều này sẽ tránh lỗi khi người dùng có quyền ghi vào thư mục của họ nhưng chroot\_local\_user=YES được kích hoạt.

**chroot\_list\_file=/etc/vsftpd/chroot\_list**:

* Chỉ định đường dẫn tệp chứa danh sách các người dùng ngoại lệ không bị chroot.

**listen=YES**:

* Kích hoạt máy chủ FTP chạy ở chế độ độc lập, lắng nghe kết nối trên các socket IPv4.

**listen\_ipv6=NO**:

* Vô hiệu hóa việc lắng nghe kết nối trên các socket IPv6.

**pam\_service\_name=vsftpd**:

* Chỉ định tên dịch vụ PAM (Pluggable Authentication Modules) cho VSFTPD, sử dụng các thiết lập bảo mật xác thực trong /etc/pam.d/vsftpd.

**userlist\_enable=YES**:

* Kích hoạt tệp user\_list để kiểm soát truy cập người dùng, cho phép chỉ những người dùng trong danh sách được phép truy cập.

**tcp\_wrappers=YES**:

* Kích hoạt hỗ trợ TCP Wrappers để kiểm soát truy cập mạng thông qua các tệp /etc/hosts.allow và /etc/hosts.deny.

**userlist\_deny=NO**:

* Khi userlist\_enable=YES và userlist\_deny=NO, chỉ những người dùng trong user\_list mới được phép đăng nhập.

**userlist\_file=/etc/vsftpd/user\_list**:

* Chỉ định đường dẫn tệp chứa danh sách người dùng được phép truy cập FTP. Kết hợp với các tùy chọn ở trên, chỉ người dùng trong tệp này được phép truy cập.

**local\_root=/var/ftp/**:

* Chỉ định thư mục gốc cho tất cả người dùng FTP trên hệ thống.

Sau khi cấu hình xong, lưu file và đóng lại.

**B2**: Tiến hành khởi chạy lại vsftpd bằng lệnh:

* **systemctl restart vsftpd**

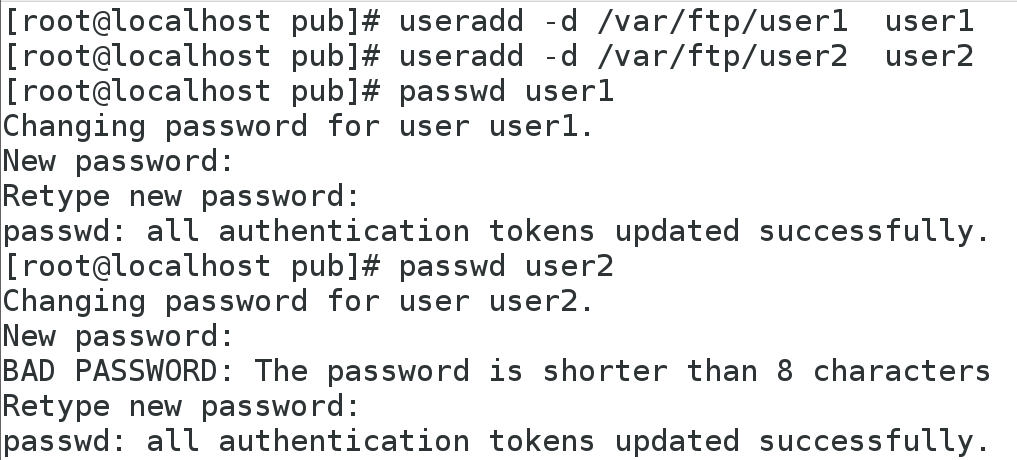
**B3**: **Tạo user** trong ftp

Ta tiến hành tạo 2 user trong ftp bằng lệnh

* **useradd -d /var/ftp/user1 user1**
* **useradd -d /var/ftp/user2 user2**

Tạo mật khẩu lần lượt cho 2 user bằng lệnh:

* **passwd user1**
* **passwd user2**



Thông tin **user1** và **user2** trong ví dụ này lần lượt là:

Name: user1 - Pass: 0823072871phuc

Name: user2 - Pass: 123456

**B4**: **Tạo nhóm quyền và phân quyền** cho 2 user vừa tạo

Tiến hành tạo 2 nhóm quyền bằng lệnh sau:

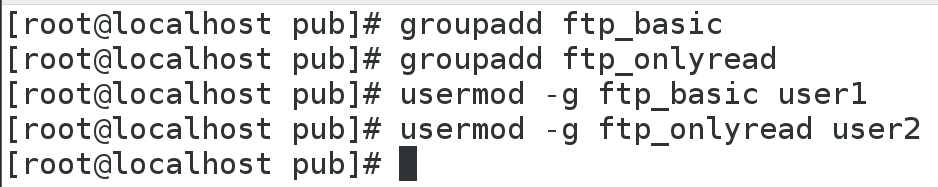
* **groupadd ftp\_basic** (nhóm quyền này sẽ có 2 quyền cơ bản đọc và ghi)
* **groupadd ftp\_onlyread** (nhóm quyền này sẽ chỉ có quyền đọc)

Gán **user1** vào nhóm quyền **ftp\_basic**

* **usermod -g ftp\_basic user1** (user1 sẽ có các quyền của nhóm ftp\_basic)

Gán **user2** vào nhóm quyền **ftp\_onlyread**

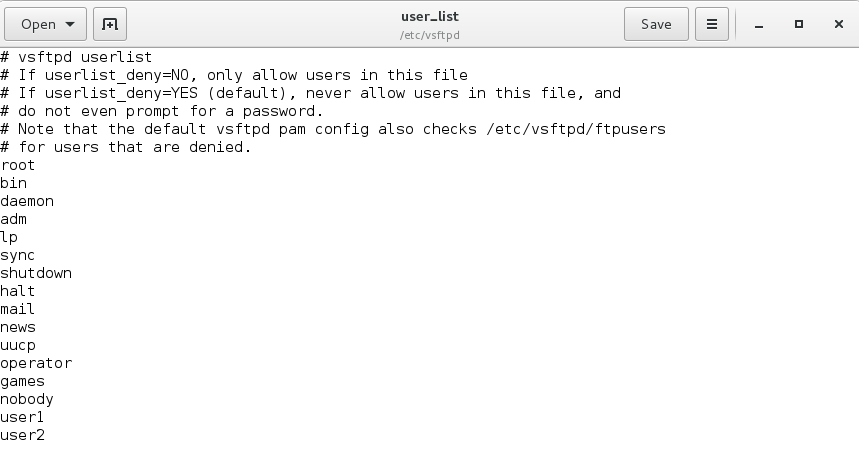
* **usermod -g ftp\_onlyread user2** (user2 sẽ chỉ có quyền đọc)



**B5**: **Thêm 2 user vào danh sách các user muốn truy cập vào ftp** bằng cách truy cập vào file user\_list:

* **gedit /etc/vsftpd/user\_list**

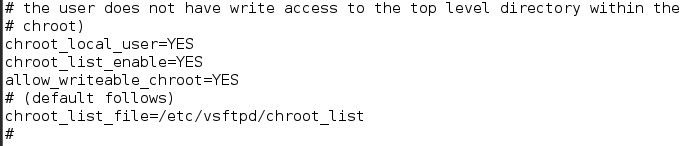
Khi đã vào được file danh sách **user\_list** của ftp, tiến hành **thêm 2 user1 và user2 vào cuối danh sách**:



**B6**: **Thêm 2 user vào file chroot.**

File **/etc/vsftpd/chroot\_list** được sử dụng để quản lý danh sách các user FTP và việc chroot của họ. Chroot là cơ chế giới hạn user trong một thư mục cụ thể, không cho phép họ truy cập ra ngoài thư mục đó.

Do ta đã cấu hình trong **file vsftpd** như bên dưới:

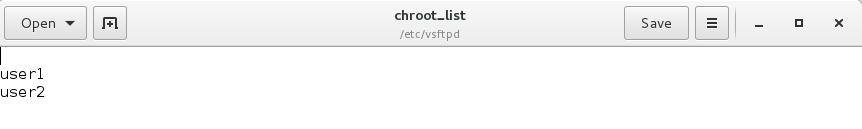


Nên tất cả user sẽ bị **chroot**, trừ những user có trong file **/etc/vsftpd/chroot\_list**

Nên giờ ta sẽ thêm user1 và user2 vào file **/etc/vsftpd/chroot\_list** để 2 user có toàn quyền truy cập.

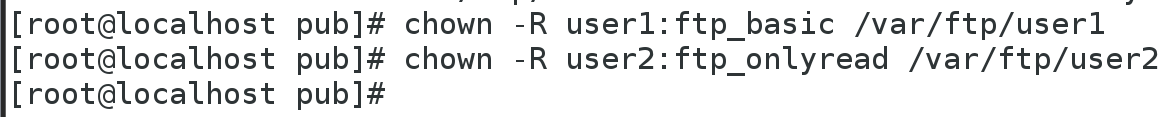
* **gedit /etc/vsftpd/chroot\_list**

Thêm 2 user1 và user2 vào:



**B7**: **Thay đổi quyền sở hữu** của 2 thư mục var/ftp/user1 và **var/ftp/user2**.

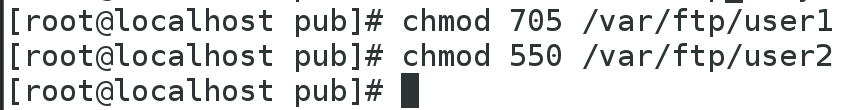
* **chown -R user1:ftp\_basic /var/ftp/user1**
  + **user1:ftp\_basic**: Thay đổi chủ sở hữu của thư mục /var/ftp/user1 thành người dùng user1 và nhóm ftp\_basic.
  + **gán chủ sở hữu của thư mục user1 là tài khoản user1**
  + **-R**: Thực hiện đệ quy, tức là áp dụng thay đổi cho tất cả các tệp và thư mục con bên trong /var/ftp/user1.
* **chown -R user2:ftp\_onlyread /var/ftp/user2**
  + **user2:ftp\_onlyread**: Thay đổi chủ sở hữu của thư mục /var/ftp/user2 thành người dùng user2 và nhóm ftp\_onlyread.
  + **-R**: Áp dụng đệ quy cho tất cả các tệp và thư mục con bên trong /var/ftp/user2.



**B8**: **Thay đổi quyền truy cập** của thư mục **/var/ftp/user1** và **/var/ftp/user2**

Lệnh **chmod** được sử dụng để thay đổi quyền truy cập của tệp hoặc thư mục. Trong lệnh này, các quyền được biểu diễn dưới dạng số

* **chmod 705 /var/ftp/user1 (Cho phép chủ sở hữu có toàn quyền, người khác chỉ có thể đọc và thực thi)**
  + **705**: Quyền cho thư mục /var/ftp/user1 được đặt như sau:
    - **7 (Chủ sở hữu)**: Quyền đọc, ghi, và thực thi (4 + 2 + 1 = 7).
    - **0 (Nhóm)**: Không có quyền nào (không đọc, không ghi, không thực thi).
    - **5 (Người khác)**: Quyền đọc và thực thi (4 + 1 = 5).
    - **Ý nghĩa**: Chủ sở hữu (có thể là user1) có toàn quyền (đọc, ghi, thực thi) trên thư mục, trong khi nhóm không có quyền truy cập nào và người dùng khác chỉ có thể đọc và thực thi (nhưng không ghi).
* **chmod 550 /var/ftp/user2 (Chủ sở hữu và nhóm có quyền đọc và thực thi, người khác không có quyền truy cập.)**
  + **550**: Quyền cho thư mục /var/ftp/user2 được đặt như sau:
    - **5 (Chủ sở hữu):** Quyền đọc và thực thi (4 + 1 = 5).
    - **5 (Nhóm):** Quyền đọc và thực thi (4 + 1 = 5).
    - **0 (Người khác)**: Không có quyền truy cập nào.
    - **Ý nghĩa:** Chủ sở hữu và nhóm có quyền đọc và thực thi nhưng không thể ghi vào thư mục, còn người dùng khác không có quyền truy cập nào.



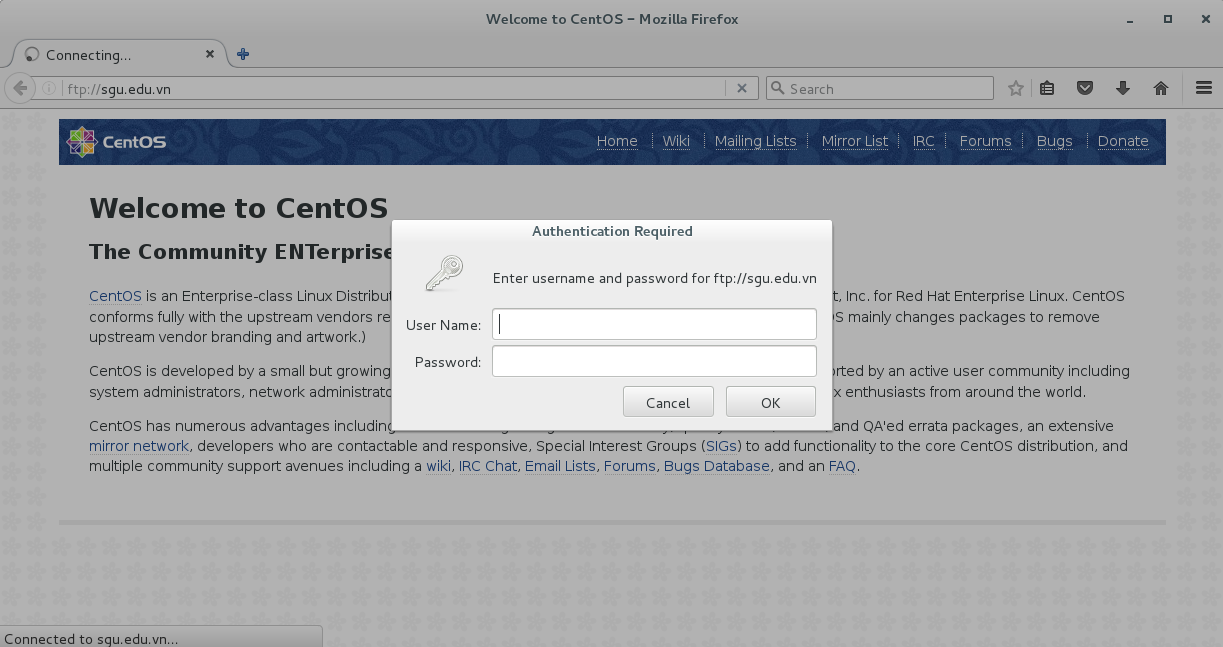
**B9: Khởi động lại vsftpd**

* **systemctl restart vsftpd**

**B10**: Tiến hành kiểm tra kết quả

Vào **Mozilla FireFox**, truy cập đường dẫn “**ftp://sgu.edu.vn/**”

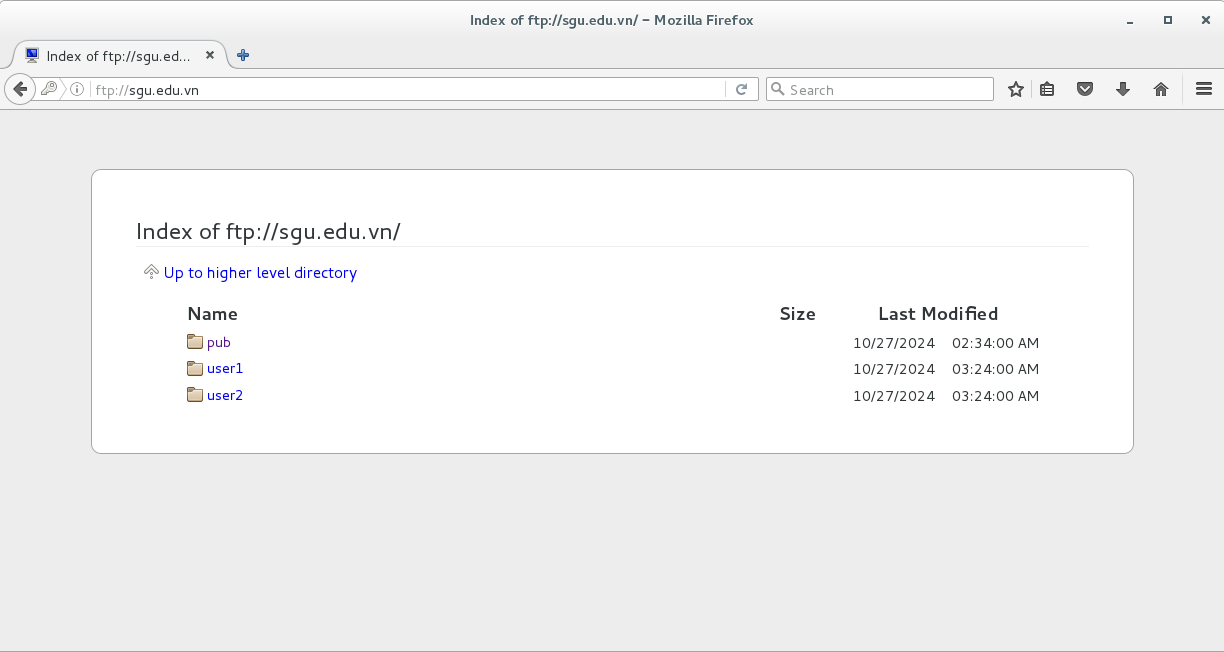
Nó sẽ bắt ta nhập username và password.



Tại đây ta tiến hành nhập thông tin user1 như ta đã thiết lập bên trên

* **User Name**: user1
* **Password**: 0823072871phuc

Ta sẽ truy cập được:

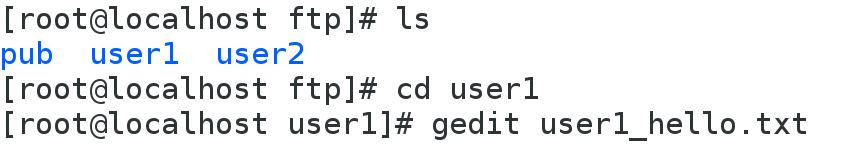


Ta có thể truy cập các thư mục trong ftp bằng lệnh

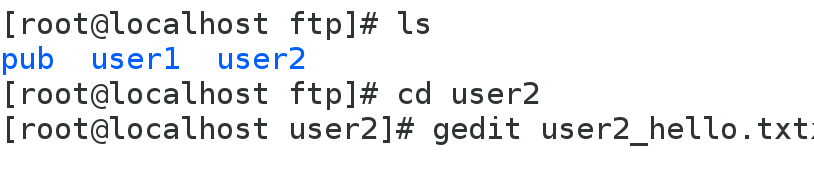
* **cd /var/ftp**

Truy cập thư mục **user1** và **user2**, ta sẽ thấy nó đang rỗng. Lần lượt tạo 2 file **user1\_hello.txt** đặt trong thư mục **user1** và **hello\_user2.txt** nằm trong thư mục **user2**

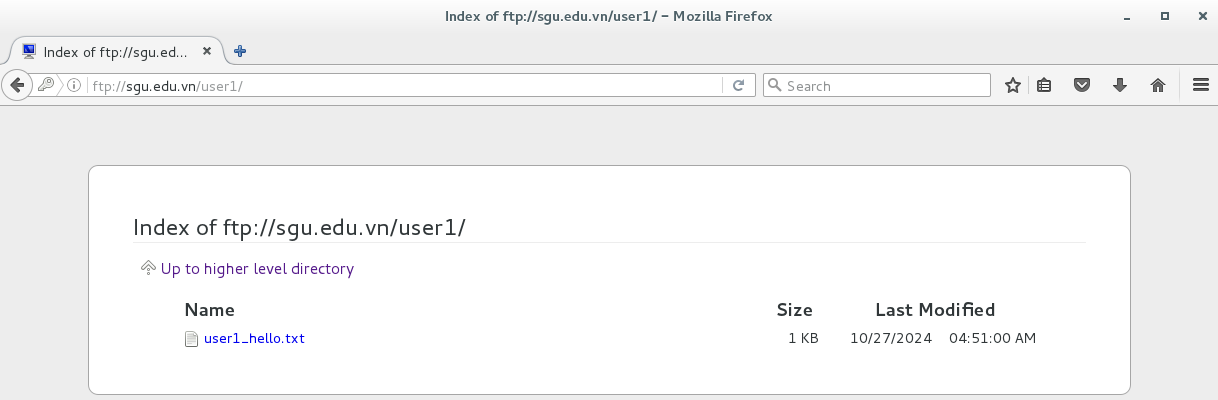
* Tạo file **user1\_hello.txt** trong thư mục **user1**

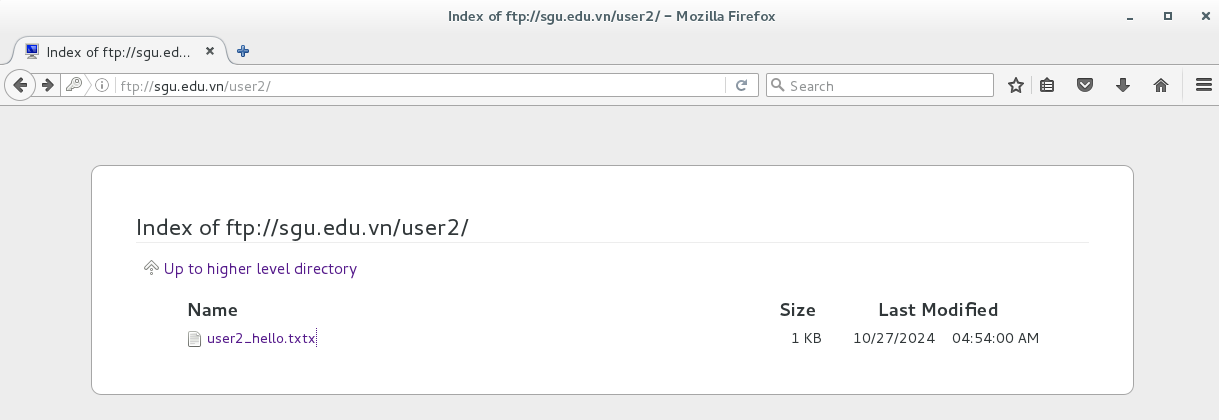


* Tạo file **user2\_hello.txt** trong thư mục **user2**



Truy cập lại “**ftp://sgu.edu.vn/**” và đăng nhập **user2** vào để kiểm tra.





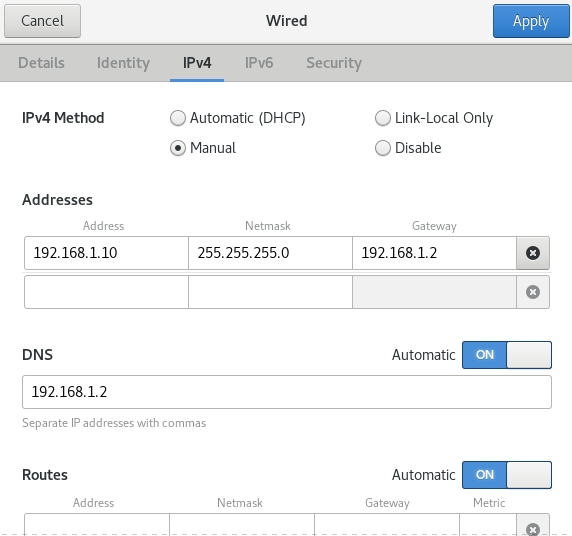
# 

# **DÙNG MỘT MÁY CENTOS CLIENT ĐỂ ĐĂNG NHẬP VÀO FTP BÊN MÁY CENTOS SERVER VÀ TẢI FILE**

Những thiết lập của phần “[**KHỞI CHẠY FTP VỚI USER**](#_cslrz5kl3z59)” là thiết lập cho bên **CentOS Server**. Giờ ta tiến hành tạo một máy CentOS Client để đăng nhập vào ftp bên CentOS Server.

**Các bước để thực hiện**:

**B1**: **Cấu hình IP tĩnh bên CentOS Client.** Ta tiến hành thiết lập IP trên máy CentOS Client để máy có thể phân giải được tên miền “sgu.edu.vn”:



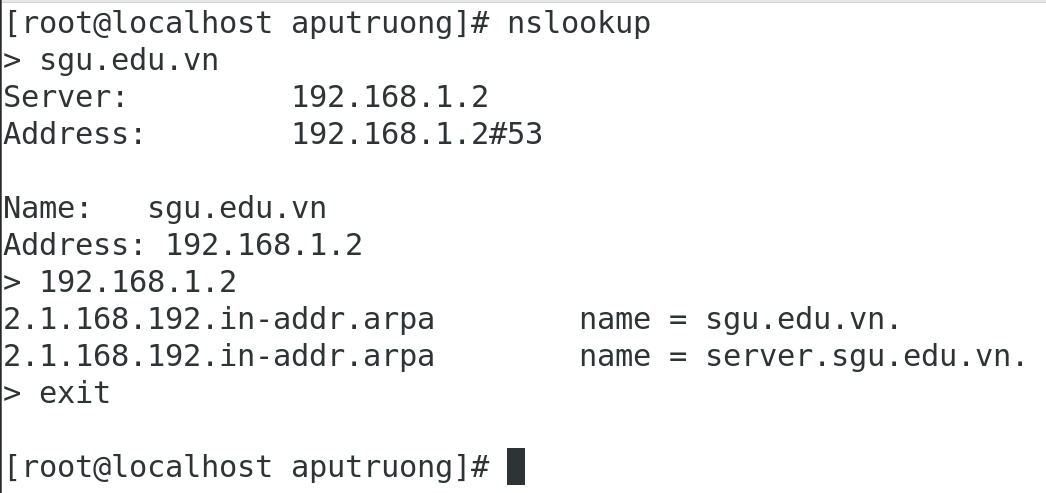
**Lưu ý: Phần DNS thiết lập trỏ đến IP của máy Server.**

Kiểm tra trong thư mục **resolv.conf**

* **gedit /etc/resolv.conf**

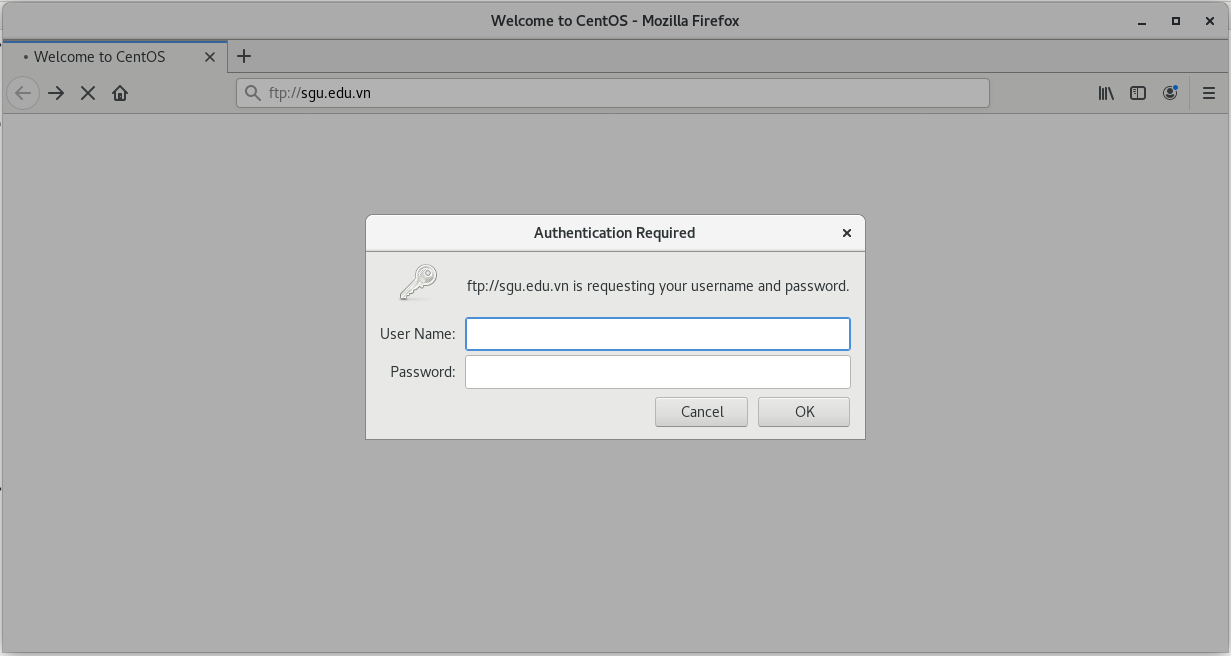


Sau khi thiết lập xong, ta tiến hành dùng lệnh **nslookup** xem máy Client có phân giải được tên miền **sgu.edu.vn** chưa. **Lưu ý**: trên máy Client cũng phải [**cài gói BIND**](#_jsn2qmw43i9n) mới có thể dùng được lệnh **nslookup** CentOS Client.



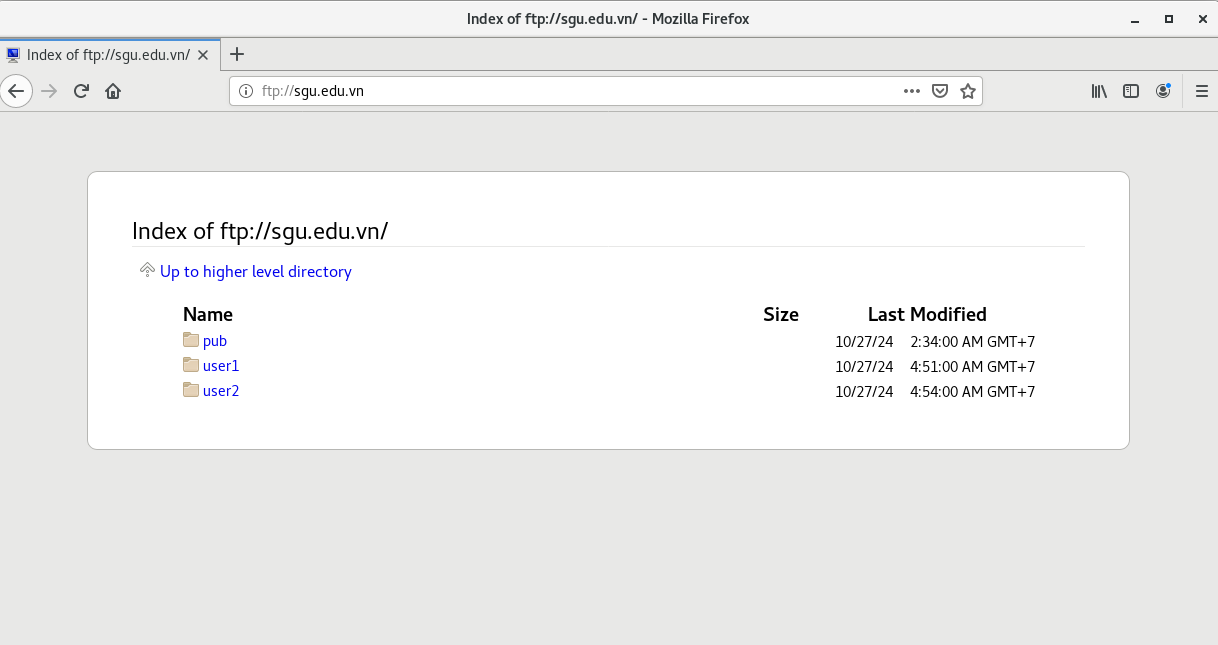
Nếu kết quả của máy Client được kết quả như trên thì đã thành công.

**B2**: Trên máy **Client**, ta **mở Mozilla FireFox và truy cập vào đường dẫn “ftp://sgu.edu.vn”**, lúc này nó sẽ yêu cầu ta đăng nhập:

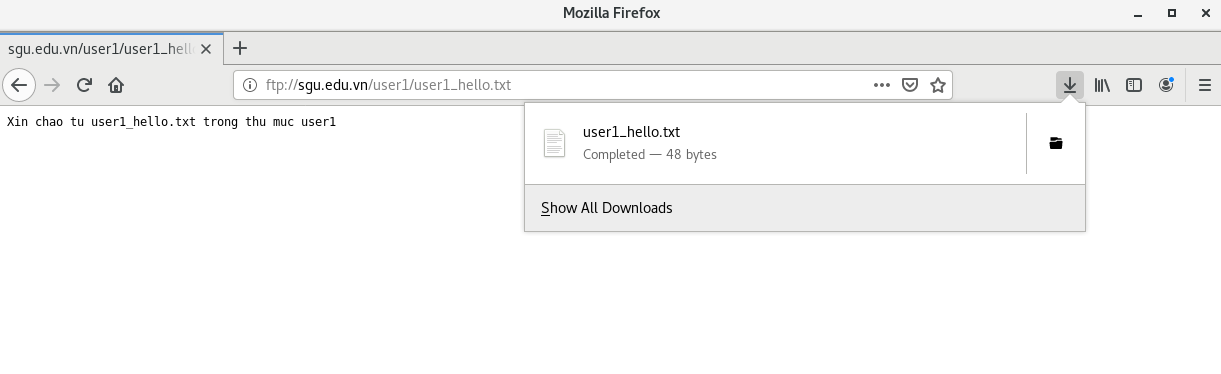


Ta tiến hành đăng nhập bằng tài khoản **user2** như đã thiết lập bên máy Server

* User Name: user2
* Passowrd: 123456



Ta có thể tải các file nằm trong thư mục **user1** và **user2** về máy của **Client**:



# **DÙNG MỘT MÁY CENTOS CLIENT ĐỂ ĐĂNG NHẬP VÀO FTP BÊN MÁY CENTOS SERVER VÀ THỰC HIỆN VIỆC THÊM FILE bằng công cụ “lftp”**

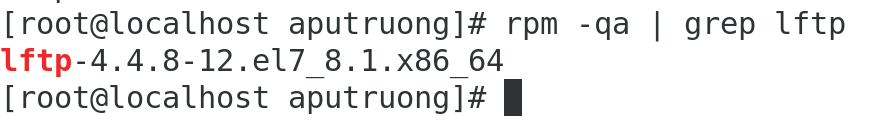
**“lftp”** là **một công cụ dòng lệnh mạnh mẽ** dùng để truyền tải tệp qua mạng với các giao thức như FTP (File Transfer Protocol), FTPS (FTP Secure), SFTP (SSH File Transfer Protocol), HTTP, HTTPS, và một số giao thức khác. Nó có thể được sử dụng để kết nối đến các máy chủ từ xa và thực hiện các thao tác trên tệp như tải lên, tải xuống, duyệt thư mục, và đồng bộ thư mục.

Và để tải được **lftp**, bạn cần phải thay đổi đường dẫn repo tải của CentOS như những phần trước:

* B1: gõ lệnh “**gedit /etc/yum.repos.d/CentOS-Base.repo**” để vào cấu hình file.
* B2: Tìm tất cả các dòng bắt đầu bằng “**mirrorlist=”** và thêm dấu **#** trước chúng để vô hiệu hóa. Sau đó, tìm dòng bắt đầu bằng “**baseurl=”** và cập nhật lại như sau:

**baseurl=http://vault.centos.org/7.9.2009/os/$basearch/**

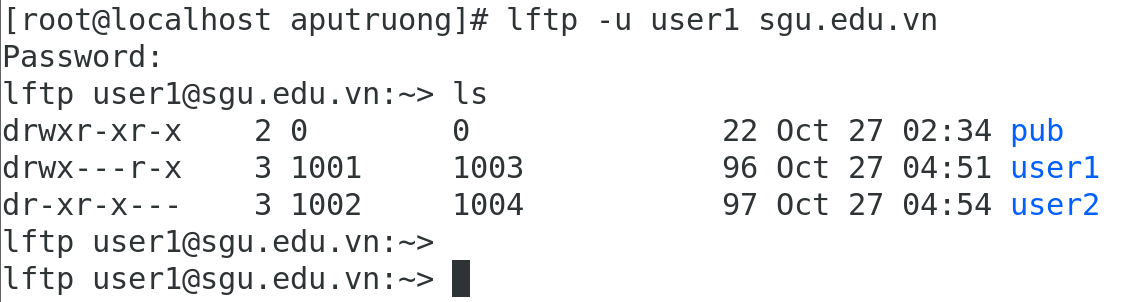
* B3: sau khi sửa xong, lưu file lại và tiến hành tải gói **lftp** về bằng lệnh “**yum install lftp -y**” (lưu ý: cần kiểm tra kết nối mạng trước khi tải bằng lệnh ping 8.8.8.8)
* B4: Sau khi tải xong, ta có thể kiểm tra xem đã có lftp trên máy chưa bằng lệnh.
  + **rpm -qa | grep lftp**



Giờ ta tiến hành truy cập FTP Server trên máy Client bằng tài khoản **user1** bằng lệnh sau:

* **lftp -u user1 sgu.edu.vn**

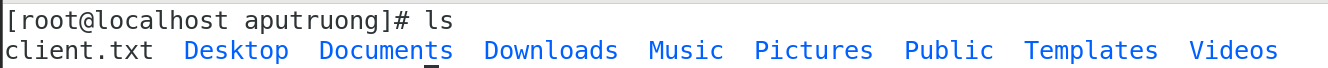
Và tiến hành nhập password như đã thiết lập trên máy Server. Ta sẽ được kết quả như bên dưới:

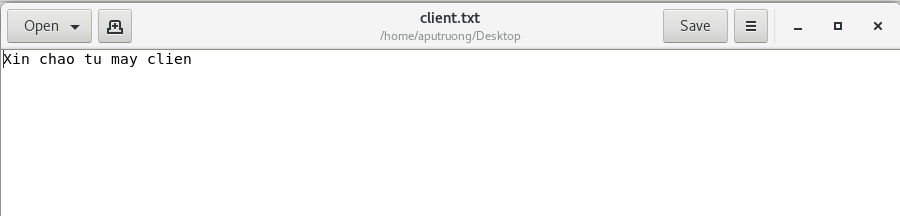


**Và giờ ta sẽ tiến hành đẩy một file từ máy Client lên FTP Server.**

Các bước để tạo một file trong máy Client và đẩy lên FTP Server

**B1**: Tạo một file **client.txt** trong máy Client.

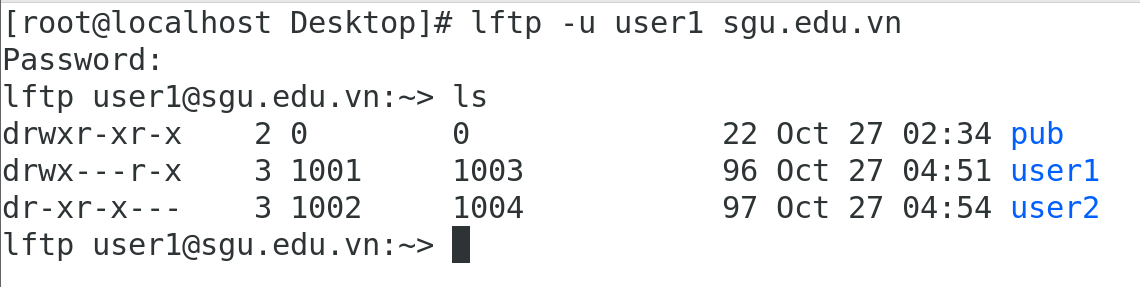




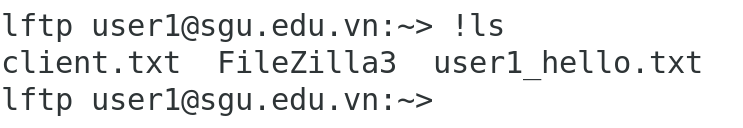
**B2**: Giờ ta tiến hành truy cập FTP bằng **lftp**:

* **lftp -u user1 sgu.edu.vn**

Dùng lệnh **ls** để kiểm tra các file có trên FTP Server



Giờ ta dùng lệnh **!ls** để kiểm tra các file có trên máy Client



Ta sẽ thấy có 3 file, trong đó:

* File “**client.txt**” ta vừa mới tạo bên trên.
* File “**user1\_hello.txt**” là file ta vừa mới tải từ FTP Server về. (trong phần “[**DÙNG MỘT MÁY CENTOS CLIENT ĐỂ ĐĂNG NHẬP VÀO FTP BÊN MÁY CENTOS SERVER VÀ TẢI FILE**](#_m4eukp5tzlbr)”)

**B3 (quan trọng)**: **tắt SELinux cả 2 phía Server và Client**, vì nó có thể cản trở quyền put file của client.

SELinux (Security-Enhanced Linux) là một mô-đun bảo mật được tích hợp vào nhân Linux, được phát triển bởi NSA (Cơ quan An ninh Quốc gia Hoa Kỳ). Nó cung cấp một lớp bảo mật bổ sung bên cạnh các cơ chế bảo mật truyền thống của Linux.

Các điểm chính về SELinux:

1. Cơ chế hoạt động:

* Dựa trên nguyên tắc MAC (Mandatory Access Control)
* Kiểm soát quyền truy cập dựa trên chính sách (policy)
* Mọi tiến trình và tệp tin đều được gán nhãn bảo mật

1. Các chế độ hoạt động:

* Enforcing: Thực thi các chính sách bảo mật
* Permissive: Chỉ ghi log vi phạm, không chặn
* Disabled: Tắt hoàn toàn SELinux

1. Lợi ích chính:

* Bảo vệ hệ thống khỏi các phần mềm độc hại
* Ngăn chặn các tiến trình truy cập trái phép
* Giảm thiểu tác động của các lỗ hổng bảo mật
* **sudo setenforce 0**

**B4**: Đẩy file “**client.txt**” từ Client lên FTP Server.

Ta tiến hành đi đến thư mục user1.

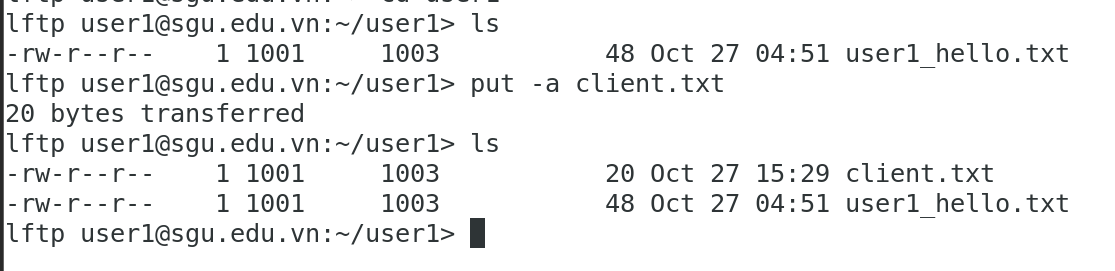
* **cd user1**



Như ta thấy bên trên, khi dùng lệnh ls để kiểm tra các file có trong thư mục user1 bao gồm file **user1\_hello.txt** được tải lên từ phía Server.

Giờ ta tiến hành đẩy file client.txt lên bằng lệnh

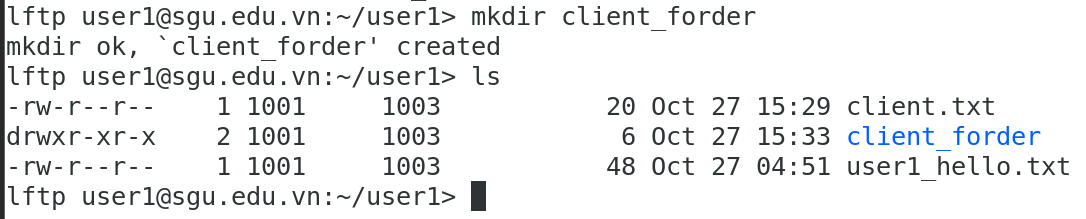
* **put -a client.txt**



Sau khi put file lên, ta tiến hành kiểm tra lại bằng lệnh ls, lúc này trong thư mục user1 sẽ có thêm một file client.txt do phía client vừa đẩy lên.

Không chỉ đẩy file lên, ta có thể tạo một folder trong thư mục user1 bằng lệnh

* **mkdir client\_folder**

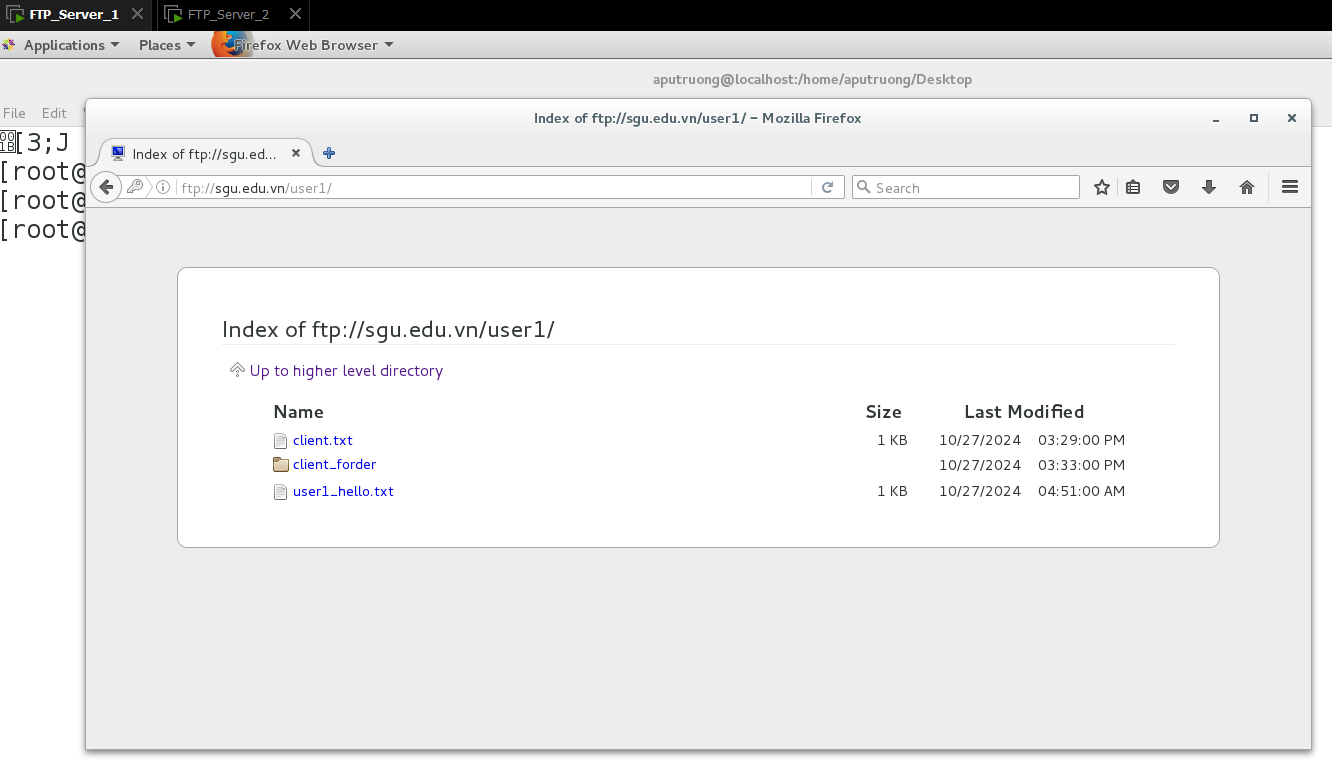


Ta cũng có thể xóa một file ra khỏi user1 bằng lệnh

* **rm <tên\_file>**

**B5**: Kiểm tra trên máy Server xem có thấy thư mục và tệp mà Client đưa lên không.

Mở Mozilla FireFox và truy cập đường dẫn “ftp://sgu.edu.vn/” và đăng nhập user1 vào.



Nếu kết quả như trên thì bạn đã thành công

# **Cài đặt FILEZILLA trên máy CLIENT**

Ngoài **lftp** ra thì chúng ta có thể dùng **filezilla** với giao diện thân thiện hơn công cụ dòng lệnh **lftp**

**Các bước để cài đặt**

**Bước 1: Kiểm tra và cập nhật hệ thống**

Trước tiên, hãy đảm bảo hệ thống của bạn được cập nhật bằng cách chạy:

* **sudo yum update -y**

**Bước 2: Cài đặt EPEL Repository**

Vì FileZilla không có sẵn trong kho chính của CentOS 7, bạn cần cài đặt **EPEL Repository** để truy cập nhiều gói phần mềm hơn.

* **sudo yum install epel-release -y**

**hoặc**

* **yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm -y**

**Bước 3: Cài đặt Filezilla**

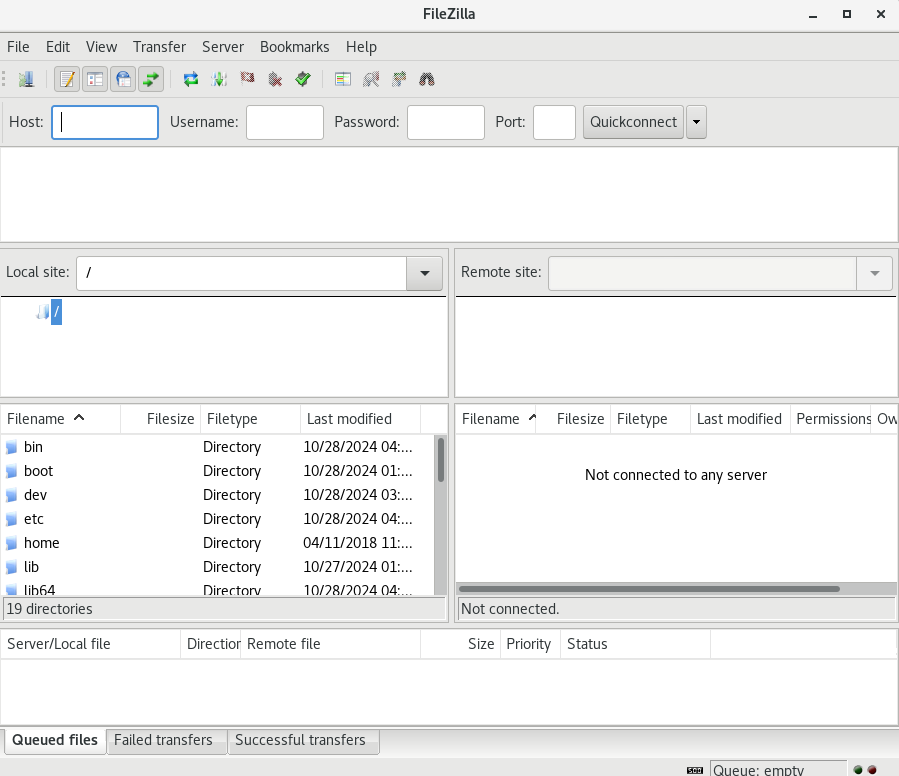
* **sudo yum install filezilla -y**

**Bước 4: Khởi động lại D-Bus**

* **sudo systemctl restart dbus**

**Bước 5: Mở filezilla**

* **filezilla**

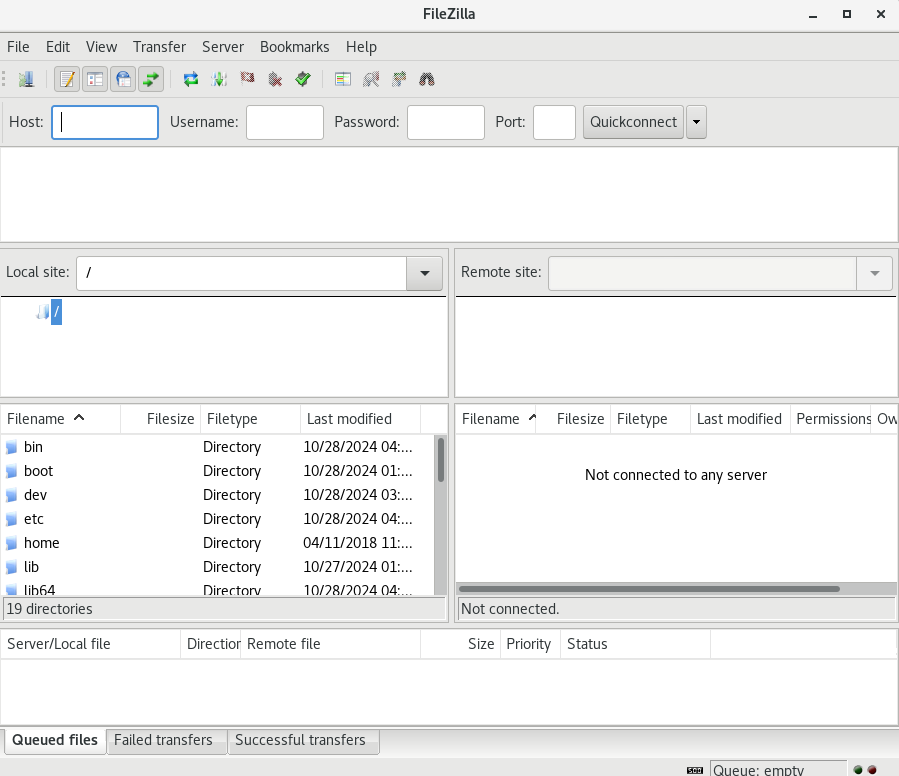
****

# **Thực hành FILEZILLA trên máy CLIENT**

Sau khi đã cài đặt thành công, ta tiến hành kết nối đến FTP Server

B1: Mở ứng dụng **filezilla** bằng dòng lệnh

* **filezilla**

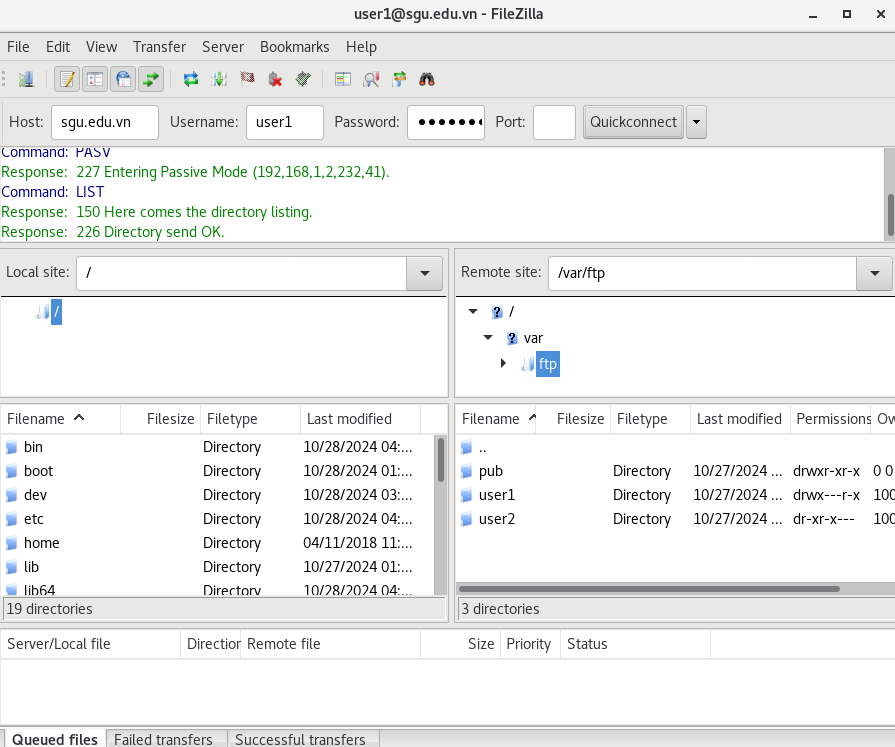
****

**B2**: Ta tiến hành nhập thông tin của phần host, Username và Password, giá trị phần port không điền để nó sử dụng mặc định

Thông tin cần điền

* **host**: sgu.edu.vn
* **Username**: user1
* **Password**: 0823072871phuc

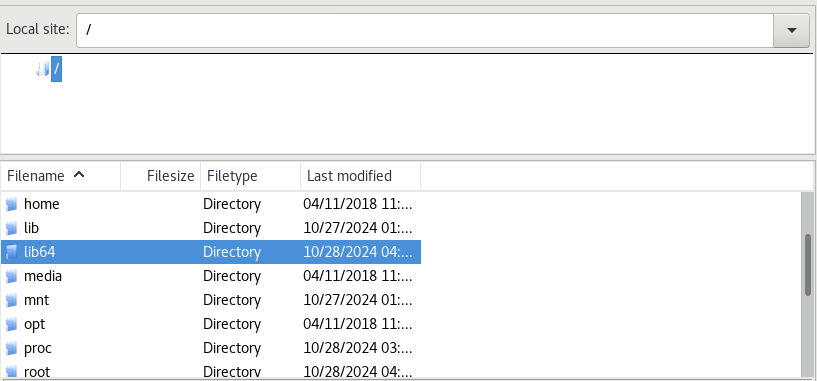
Sau khi điền xong thông tin, ta nhấn nút “**Quickconnect**” để bắt đầu kết nối.



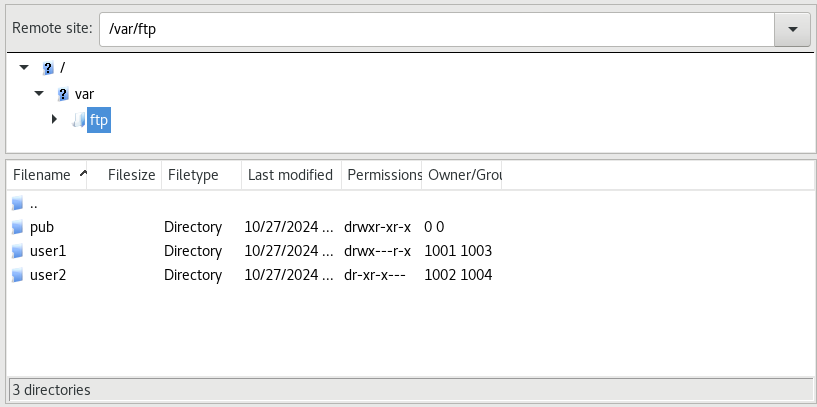
Kết quả như bên trên là đã kết nối thành công.

**Giải thích thêm các thông tin trên hình:**

Phần **Local Site** là những thư mục và file trên máy client.



Phần **Remote site** là các thư mục và file trên FTP Server

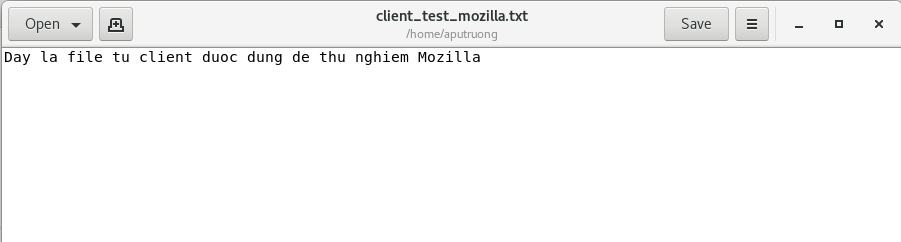


**B3**: Ta có thể thực hiện thao tác giống như thực hiện lftp

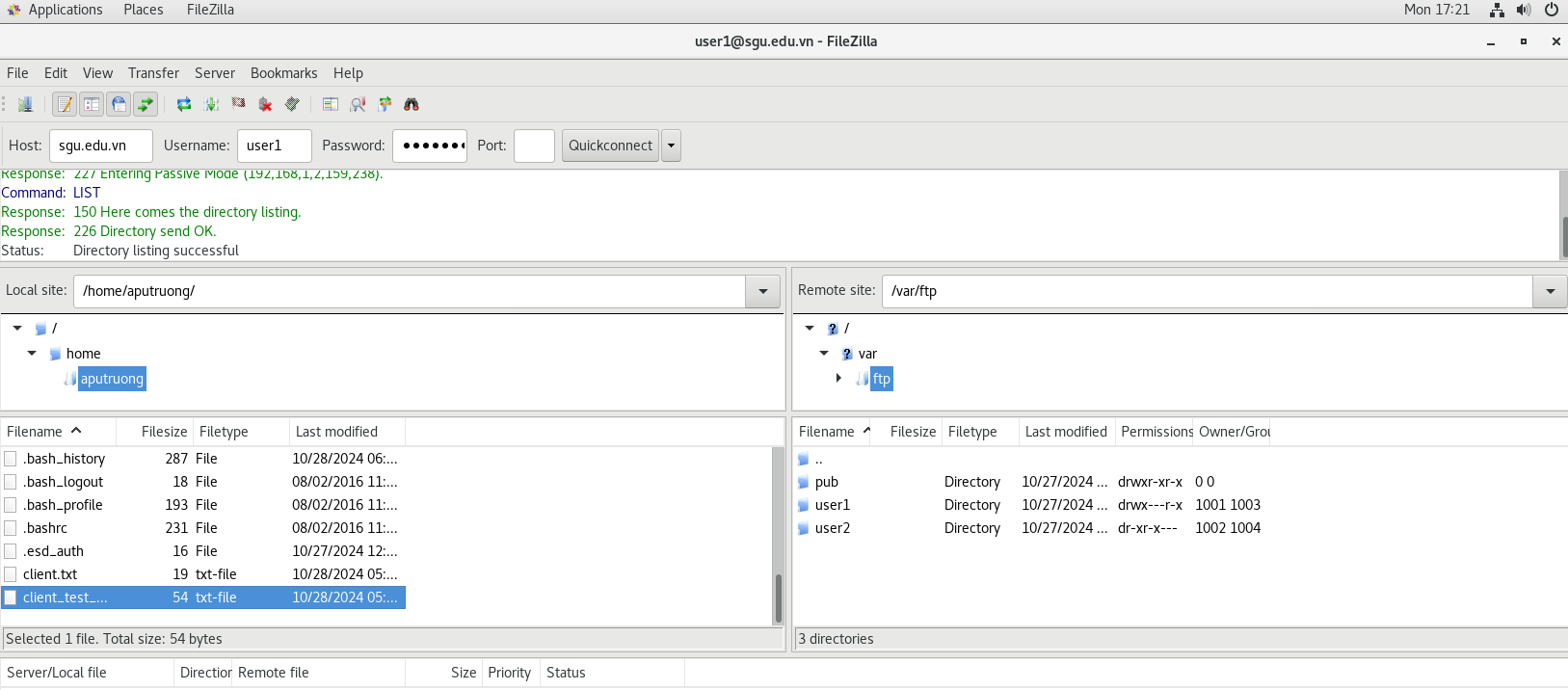
* Tạo một file trong máy client và put file lên

Tạo một file “**client\_test\_mozilla.txt**” trên máy client:

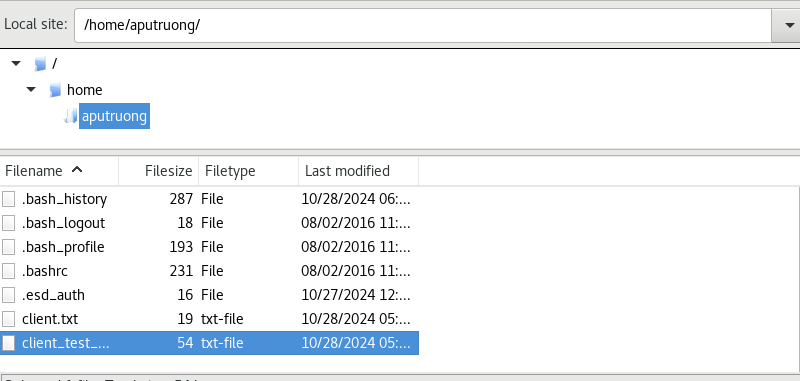




Kiểm tra lại trong ứng dụng Filezilla

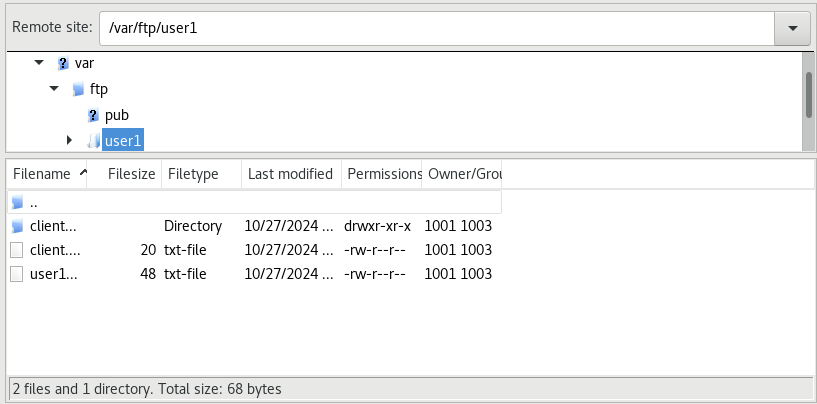


Phần Local site ta sẽ thấy file vừa mới tạo:



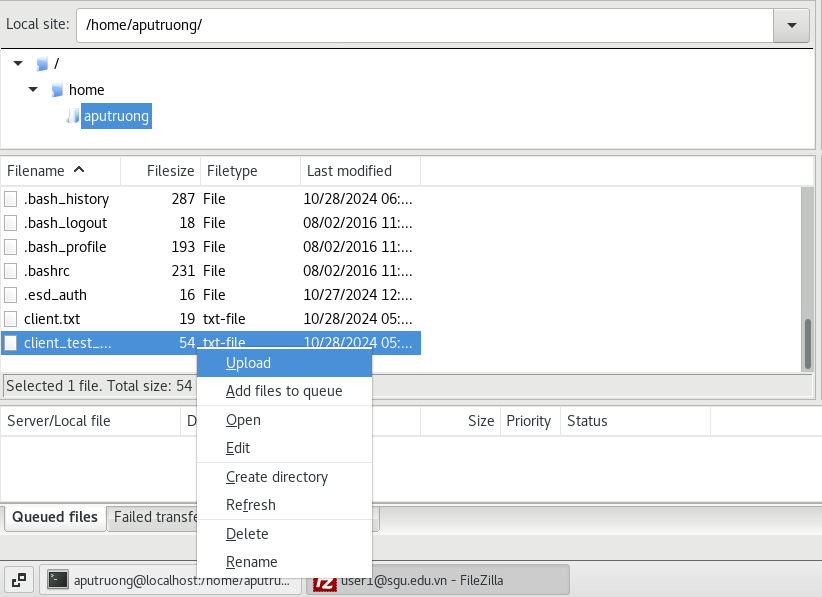
Giờ ta sẽ tiến hành put file lên bằng các thao tác sao

**B1**: bên phần **Remote site**, nơi hiển thị các file trên FTP Server, ta **di chuyển vào thư mục user1**.

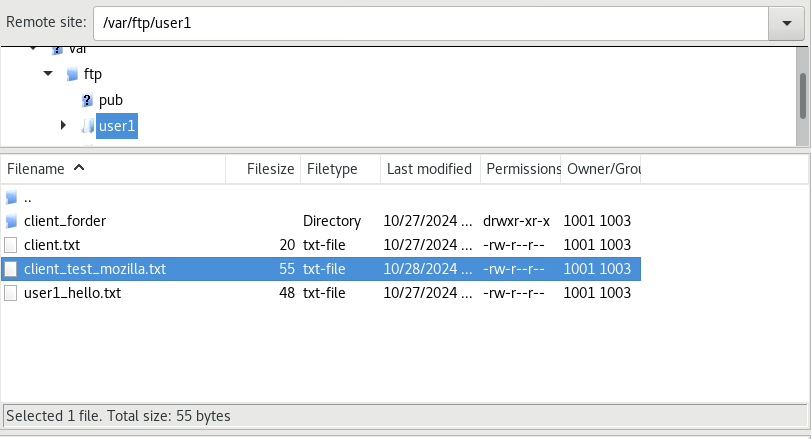


**B2**: Bên phần **Local site**

Click chuột phải vào file **client\_test\_mozilla.txt** và click chuột phải chọn **Upload**.



Nếu thành công, b**ên phần Remote Site,** trong thư mục **user1** sẽ có file ta vừa mới đưa lên



**Sử dụng lftp làm được 4 thứ:**

1. **Từ máy Client tải file từ Server về**
2. **Put file từ Client lên**
3. **Tạo file từ Client**
4. **Xóa file từ Client**
5. **lấy source web hôm nay demo lên**

**Sử dụng filezilla làm được :**

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# **DỰ ĐOÁN CÂU HỎI**

# 

Trong hệ thống Linux, quyền truy cập cho tệp và thư mục được thiết lập dựa trên ba loại quyền: **đọc (r), ghi (w) và thực thi (x)**. Các quyền này được áp dụng cho ba nhóm người dùng: **chủ sở hữu (user), nhóm (group)** và **người khác (others)**. Dưới đây là cách diễn giải các quyền này:

**1. Quyền:**

- **Đọc (r)**: Cho phép xem nội dung của tệp hoặc danh sách các tệp trong thư mục.

- **Ghi (w):** Cho phép sửa đổi nội dung của tệp hoặc thêm/xóa tệp trong thư mục.

- **Thực thi (x)**: Cho phép chạy tệp (đối với tệp thực thi) hoặc vào thư mục (đối với thư mục).

**2. Cách thiết lập quyền:**

Quyền được thiết lập bằng các ký tự sau đây:

**- u**: chủ sở hữu

**- g**: nhóm

**- o**: người khác

**- a**: tất cả (chủ sở hữu, nhóm và người khác)

**3. Ký hiệu để thiết lập quyền:**

**- r** : đọc

**- w** : ghi

**- x** : thực thi

**4. Mã số quyền (octal):**

Mỗi quyền có thể được đại diện bằng một số:

**- r : 4**

**- w : 2**

**- x : 1**

Bằng cách cộng các số này lại, bạn có thể thiết lập quyền cho chủ sở hữu, nhóm và người khác. Dưới đây là một số ví dụ:

| Quyền | Ký hiệu | Mã số |

|--------------|---------|-------|

| Không có quyền | --- | 0 |

| Chỉ thực thi | --x | 1 |

| Chỉ ghi | -w- | 2 |

| Chỉ đọc | r-- | 4 |

| Đọc + Ghi | rw- | 6 |

| Đọc + Thực thi | r-x | 5 |

| Ghi + Thực thi | -wx | 3 |

| Đọc + Ghi + Thực thi | rwx | 7 |

| Quyền | Ký hiệu | Mã số |
| --- | --- | --- |
| Không có quyền |  | 0 |
| Chỉ thực thi | --x | 1 |
| Chỉ ghi | -w- | 2 |
| Chỉ đọc | r-- | 4 |
| Đọc và ghi | rw- | 6 |
| Đọc và thực thi | r-x | 5 |
| Ghi và thực thi | -wx | 3 |
| Đọc, ghi và thực thi | rwx | 7 |

**5. Ví dụ thiết lập quyền:**

- **Chỉ cho chủ sở hữu có quyền đọc, ghi và thực thi, nhóm chỉ có quyền đọc và thực thi, và người khác không có quyền gì**:

**chmod 751 /path/to/file\_or\_directory**

- Cho tất cả quyền (đọc, ghi, thực thi) cho chủ sở hữu và nhóm, và chỉ quyền đọc cho người khác\*\*:

**chmod 775 /path/to/file\_or\_directory**

Với thông tin này, bạn có thể dễ dàng thiết lập quyền cho các tệp và thư mục trong hệ thống của mình!