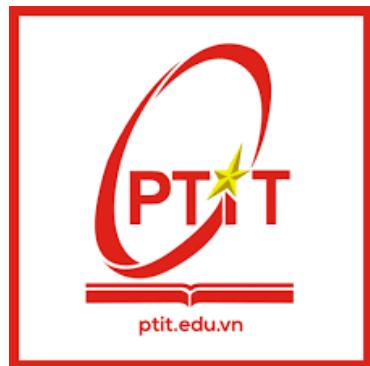


BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



Hệ điều hành window, linux

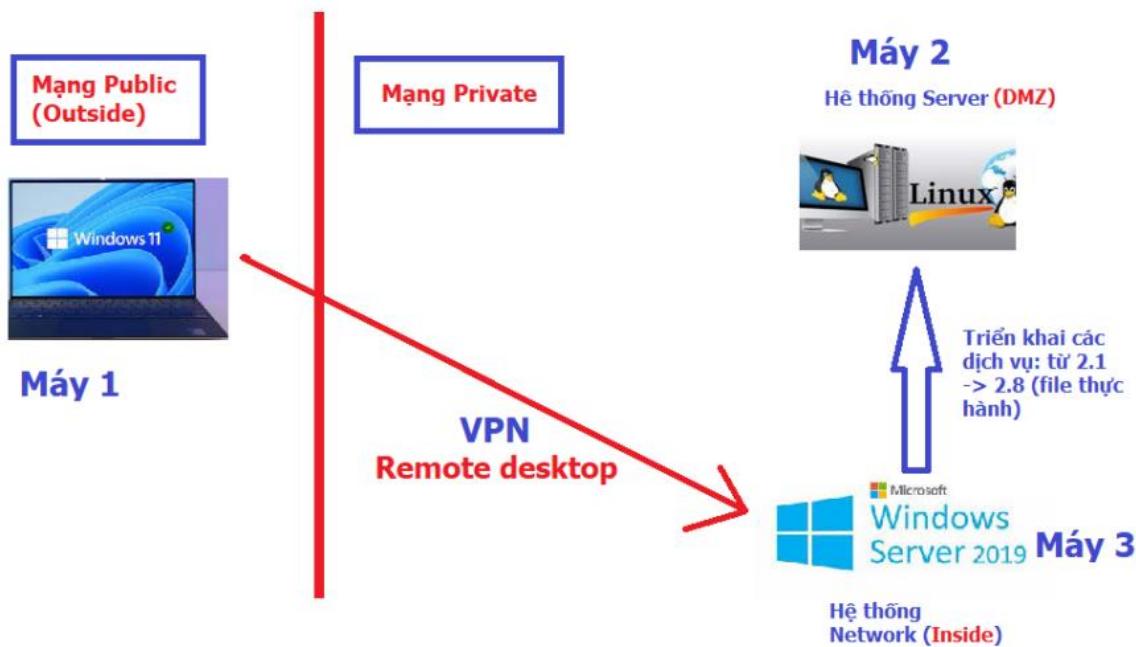
Đề tài:
TÌM HIỂU VÀ TRIỂN KHAI CÁC
DỊCH VỤ TRÊN LINUX
(UBUNTU or CentOS 7)

Người thực hiện: Nguyễn Công Lực

Mục Lục:

1. Mô hình triển khai
2. Triển khai dịch vụ
 - 2.1 Dịch vụ Truyền tin, sử dụng Giao thức TFTP, FTP,...
 - 2.2. Dịch vụ Quản trị từ xa: Remote Desktop Connection đến Server Ubuntu
 - 2.3. Dịch vụ Phân quyền User trong FTP Server
 - 2.4. Dịch vụ Quản trị từ xa
 - 2.5 Dịch vụ SSH
- 2.6. Dịch vụ DNS và DHCP
 - a. Dịch vụ DNS:
 - b. Dịch vụ DHCP:
- 2.7. Dịch vụ thư điện tử
- 2.8. Quản lý User và Group
 - a. Quản lý User
 - b. Quản lý Group
 - c. File lưu trữ dữ liệu về user và group
 - d. Sử dụng FileZilla để truy cập FTP server kiểm tra phân quyền
- 2.9. Dịch vụ web
 - * Sử dụng tool Nagios để giám sát 1 trang web, nếu bị mất liên lạc thì gửi mail để thông báo
 - a. Chuẩn bị
 - b. Cài đặt Nagios trên CentOS 7
 - c. Giám sát thông qua NRPE
 - 3. Tài liệu tham khảo

1. MÔ HÌNH TRIỂN KHAI



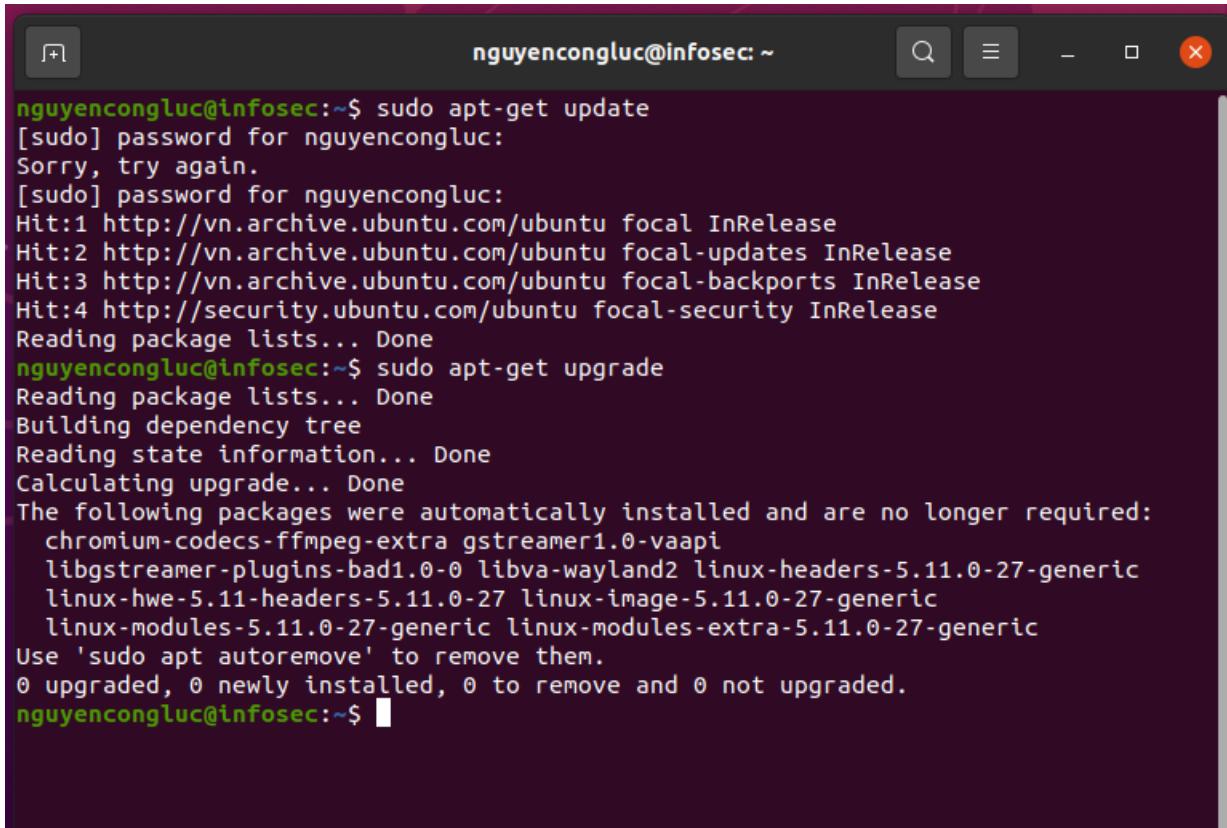
2. TRIỂN KHAI DỊCH VỤ

Lưu ý: Trong Server Ubuntu, muốn triển khai dịch vụ nào thì phải cài đặt và cấu hình loại dịch vụ tương ứng.

2.1 Dịch vụ Truyền tin, sử dụng Giao thức TFTP, FTP,...

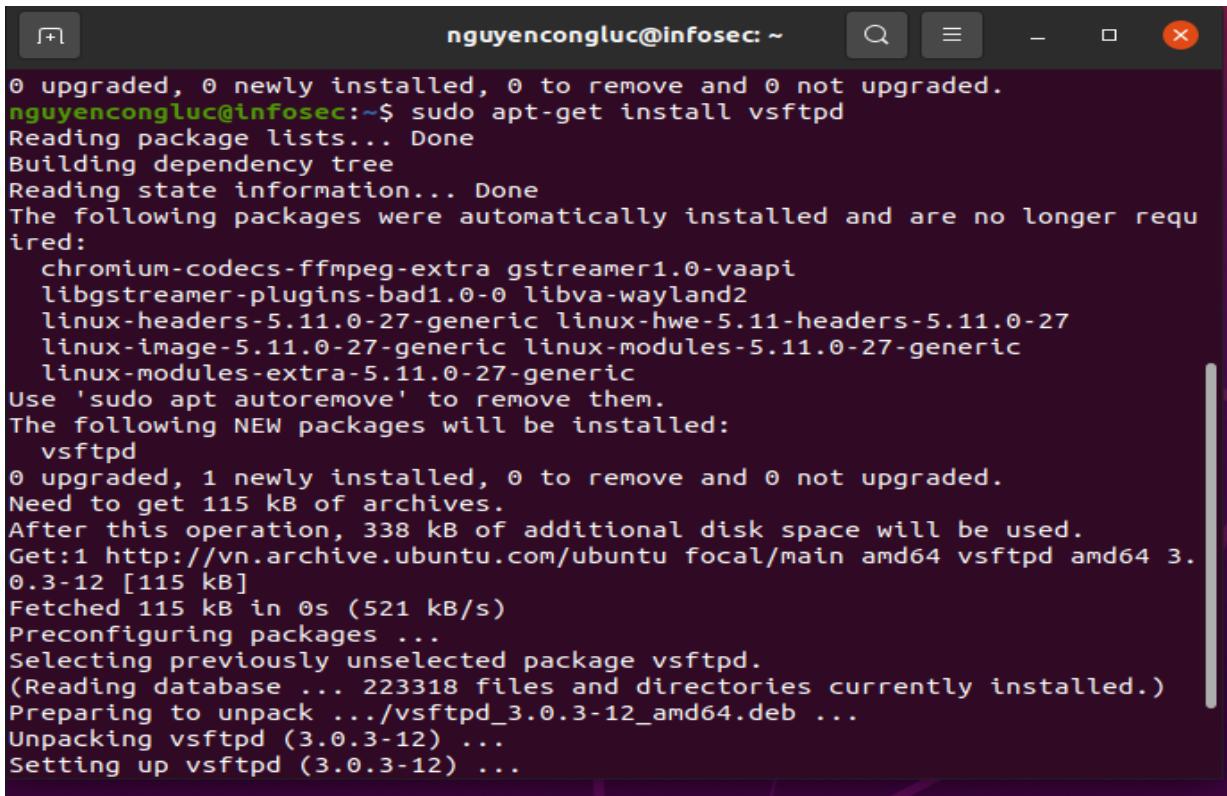
B1: Cài phần mềm FileZilla trên máy client (HĐH Win 10, hoặc Win server): trên máy thật hoặc trên máy ảo, để thực hiện kết nối với Server Ubuntu (trước khi kết nối phải sử dụng dịch vụ: VPN, AD, Domain, Vì nếu môi trường thực tế: Sử dụng từ lớp mạng bên ngoài (public) vào mạng bên trong hệ thống 1 tổ chức (Private))

B2: Cài đặt framework FTP



```
nguyencongluc@infosec:~$ sudo apt-get update
[sudo] password for nguyencongluc:
Sorry, try again.
[sudo] password for nguyencongluc:
Hit:1 http://vn.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://vn.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
nguyencongluc@infosec:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2 linux-headers-5.11.0-27-generic
  linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic
  linux-modules-5.11.0-27-generic linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
nguyencongluc@infosec:~$
```

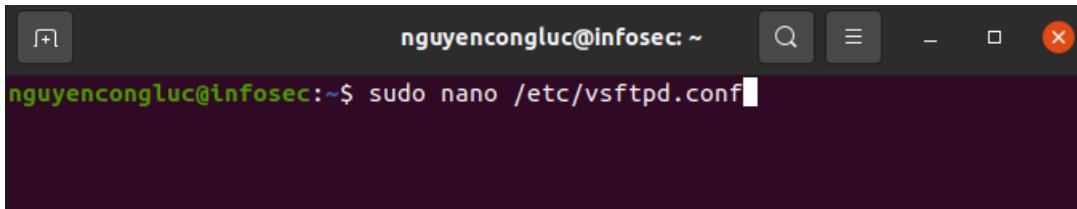
Cài đặt VSFTPD: nhập sudo apt-get install vsftpd → Enter



```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
nguyencongluc@infosec:~$ sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 115 kB of archives.
After this operation, 338 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu focal/main amd64 vsftpd amd64 3.0.3-12 [115 kB]
Fetched 115 kB in 0s (521 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 223318 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-12_amd64.deb ...
Unpacking vsftpd (3.0.3-12) ...
Setting up vsftpd (3.0.3-12) ...
```

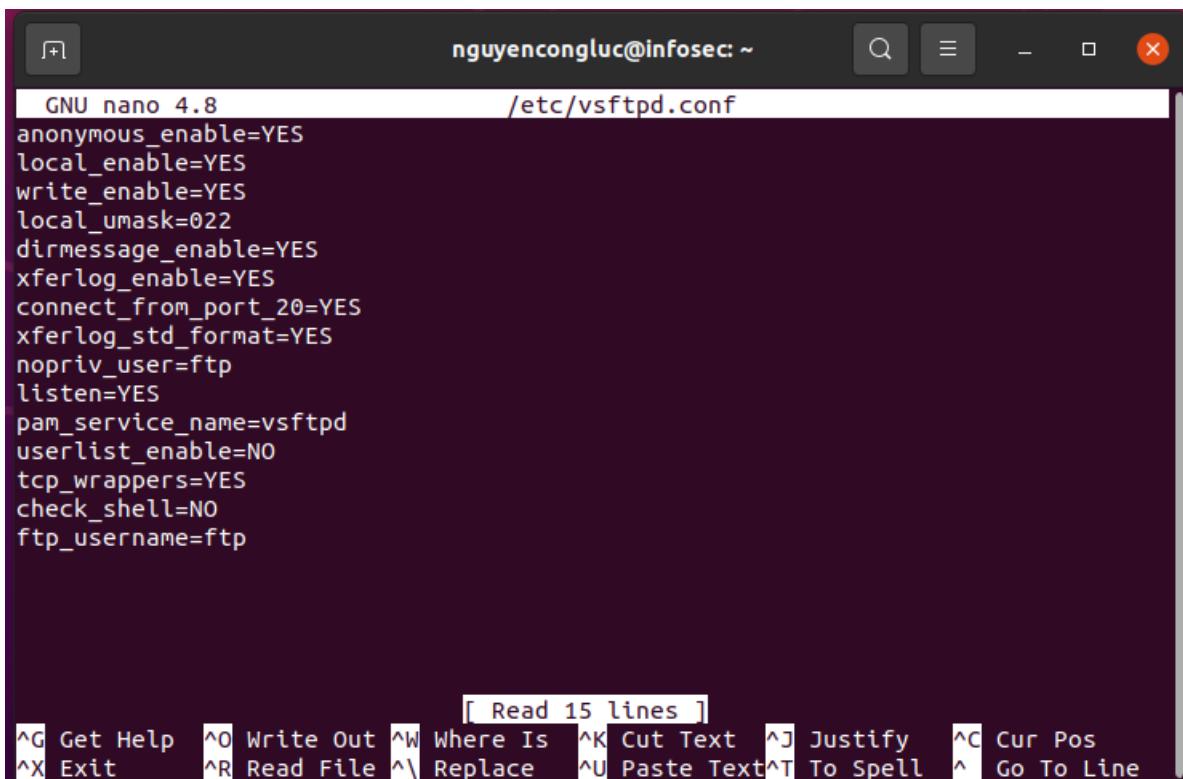
B3: cấu hình dịch vụ TFTP, FTP Trên Ubuntu Server gồm thông tin:

Mở tập tin định cấu hình VSFTPD: Nhập sudo nano /etc/vsftpd.conf



```
nguyencongluc@infosec:~$ sudo nano /etc/vsftpd.conf
```

Cấu hình:



```
GNU nano 4.8                               /etc/vsftpd.conf
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
nopriv_user=ftp
listen=YES
pam_service_name=vsftpd
userlist_enable=NO
tcp_wrappers=YES
check_shell=NO
ftp_username=ftp

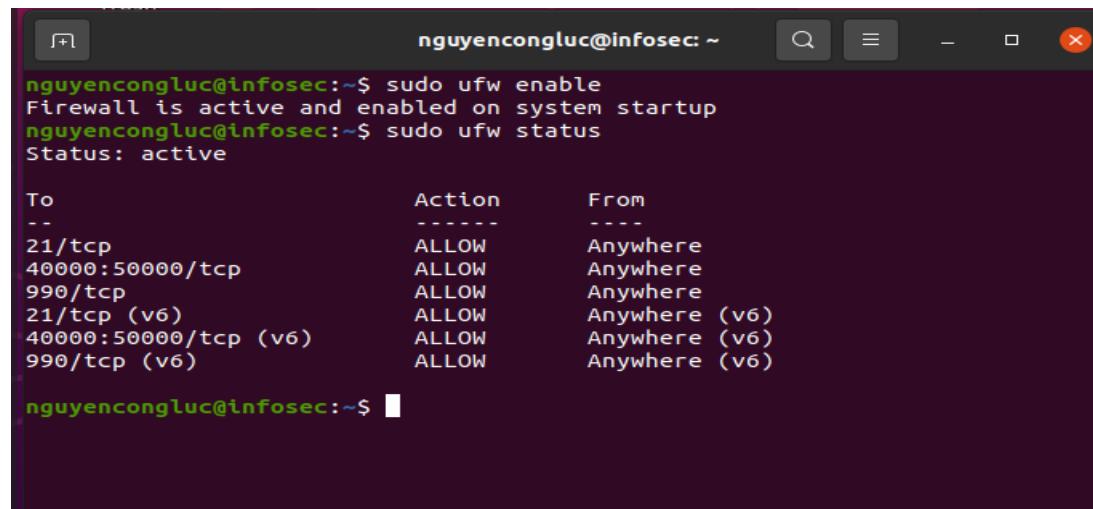
[ Read 15 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File   ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line
```

Chỉnh sửa xong thực hiện lệnh CTRL+X, Y và nhấn enter để lưu và thoát.

Mở port 20 và 21 cho FTP, port 40000 đến 50000 cho Passive FTP , port 990 cho TLS

```
nguyencongluc@infosec:~$ sudo ufw allow 21/tcp
[sudo] password for nguyencongluc:
Rules updated
Rules updated (v6)
nguyencongluc@infosec:~$ sudo ufw allow 40000:50000/tcp
Rules updated
Rules updated (v6)
nguyencongluc@infosec:~$ sudo ufw allow 990/tls
ERROR: Bad port
nguyencongluc@infosec:~$ sudo ufw allow 990/tcp
Rules updated
Rules updated (v6)
nguyencongluc@infosec:~$ sudo ufw status
Status: inactive
```

Kích hoạt firewall ufw và kiểm tra đã hoạt động



The screenshot shows a terminal window titled "nguyencongluc@infosec: ~". The user has run several commands to manage the UFW firewall:

- \$ sudo ufw enable
- Firewall is active and enabled on system startup
- \$ sudo ufw status
- Status: active

Below this, a table lists the current firewall rules:

To	Action	From
--	-----	-----
21/tcp	ALLOW	Anywhere
40000:50000/tcp	ALLOW	Anywhere
990/tcp	ALLOW	Anywhere
21/tcp (v6)	ALLOW	Anywhere (v6)
40000:50000/tcp (v6)	ALLOW	Anywhere (v6)
990/tcp (v6)	ALLOW	Anywhere (v6)

- Kiểm tra dịch vụ đã hoạt động

```
nguyencongluc@infosec:~$ sudo systemctl start vsftpd.service
nguyencongluc@infosec:~$ sudo systemctl restart vsftpd.service
nguyencongluc@infosec:~$ sudo systemctl status vsftpd.service
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-11-29 09:53:16 +07; 17s ago
     Process: 9621 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0)
    Main PID: 9622 (vsftpd)
      Tasks: 1 (limit: 2260)
     Memory: 528.0K
        CGroup: /system.slice/vsftpd.service
                  └─9622 /usr/sbin/vsftpd /etc/vsftpd.conf

Thg 11 29 09:53:16 infosec systemd[1]: Starting vsftpd FTP server...
Thg 11 29 09:53:16 infosec systemd[1]: Started vsftpd FTP server.
lines 1-12/12 (END)
```

Ảnh dưới giành cho giao diện ubuntu 16 với cấu trúc lệnh có chút thay đổi

nguyencongluc@ubuntu:~\$ 990/tcp (v6) ALLOW Anywhere (v6)

```
nguyencongluc@ubuntu:~$ sudo systemctl start vsftpd.service
sudo: systemctl: command not found
nguyencongluc@ubuntu:~$ sudo start vsftpd.service
start: Unknown job: vsftpd.service
nguyencongluc@ubuntu:~$ service vsftpd start
start: Unknown job: vsftpd
nguyencongluc@ubuntu:~$ sudo systemctl restart vsftpd
sudo: systemctl: command not found
nguyencongluc@ubuntu:~$ sudo service vsftpd start
start job is already running: vsftpd
nguyencongluc@ubuntu:~$ sudo service vsftpd status
vsftpd start/running, process 2702
nguyencongluc@ubuntu:~$ ftp 192.168.100.157
Connected to 192.168.100.157.
220 (vsFTPd 3.0.2)
Name (192.168.100.157:nguyencongluc): nguyencongluc
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Kết nối ftp

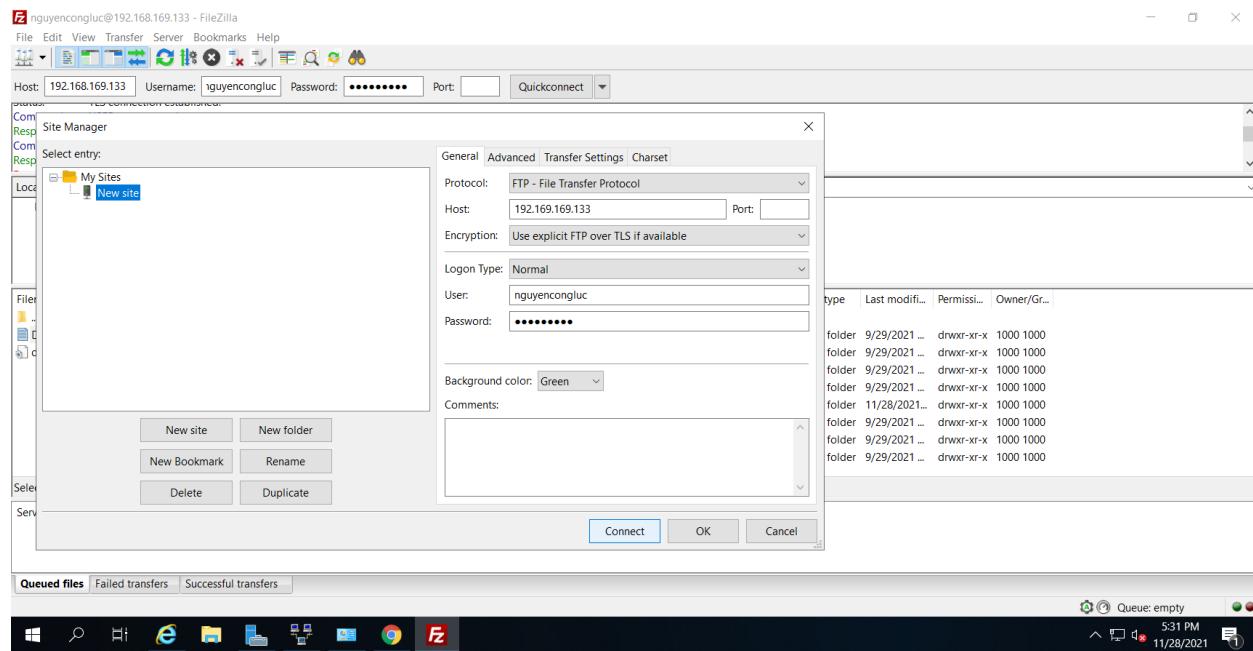
```
nguyencongluc@infosec:~$ ftp 192.168.169.133
Connected to 192.168.169.133.
220 (vsFTPD 3.0.3)
Name (192.168.169.133:nguyencongluc): nguyencongluc
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp>
```

```
C:\Windows\system32\cmd.exe - ftp 192.168.169.133
Microsoft Windows [Version 10.0.22000.318]
(c) Microsoft Corporation. All rights reserved.

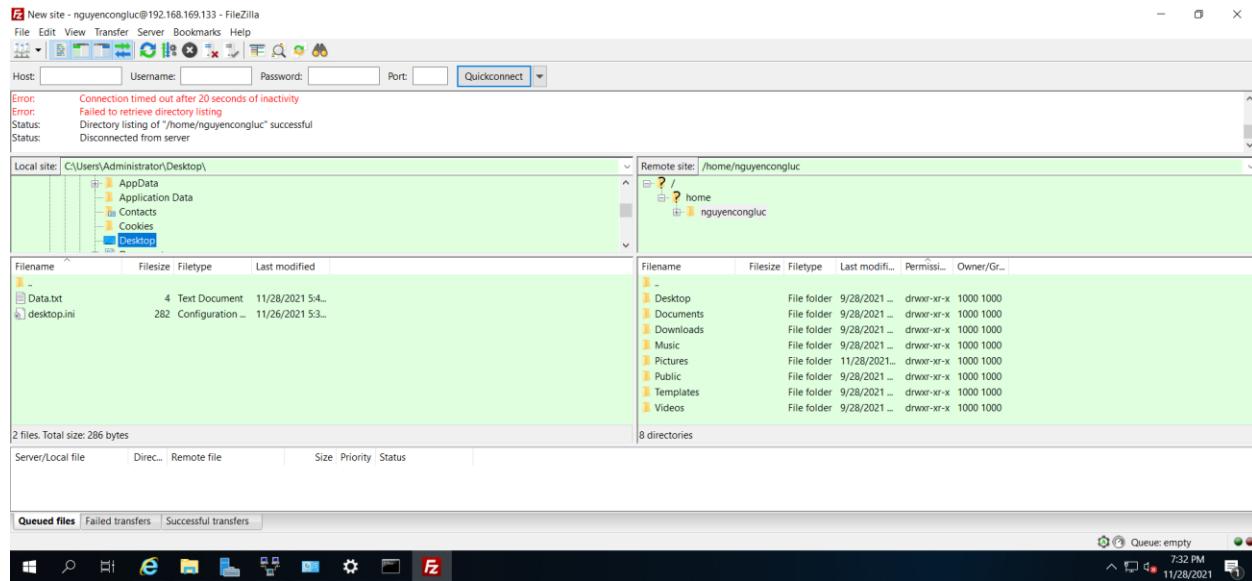
C:\Users\Nguyen Cong Luc>ftp 192.168.169.133
Connected to 192.168.169.133.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
User (192.168.169.133:(none)): nguyencongluc
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

B4: Cài phần mềm FileZilla client (trên máy cá nhân) để kết nối đến Server Ubuntu.

Ip Ubuntu server: 192.168.169.133

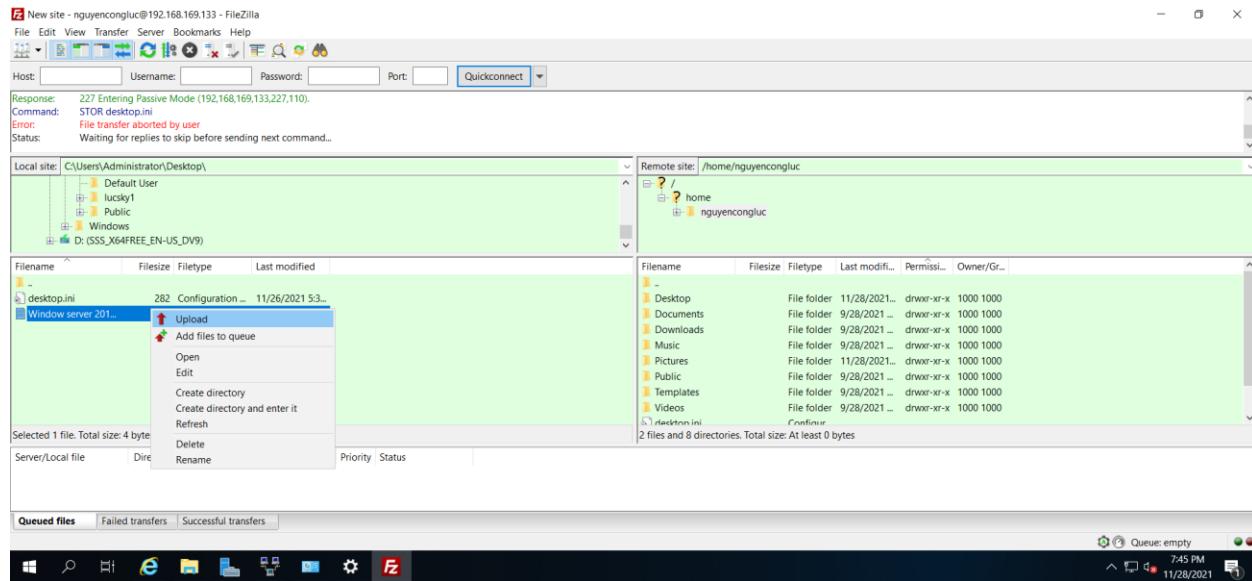


- Kết nối thành công

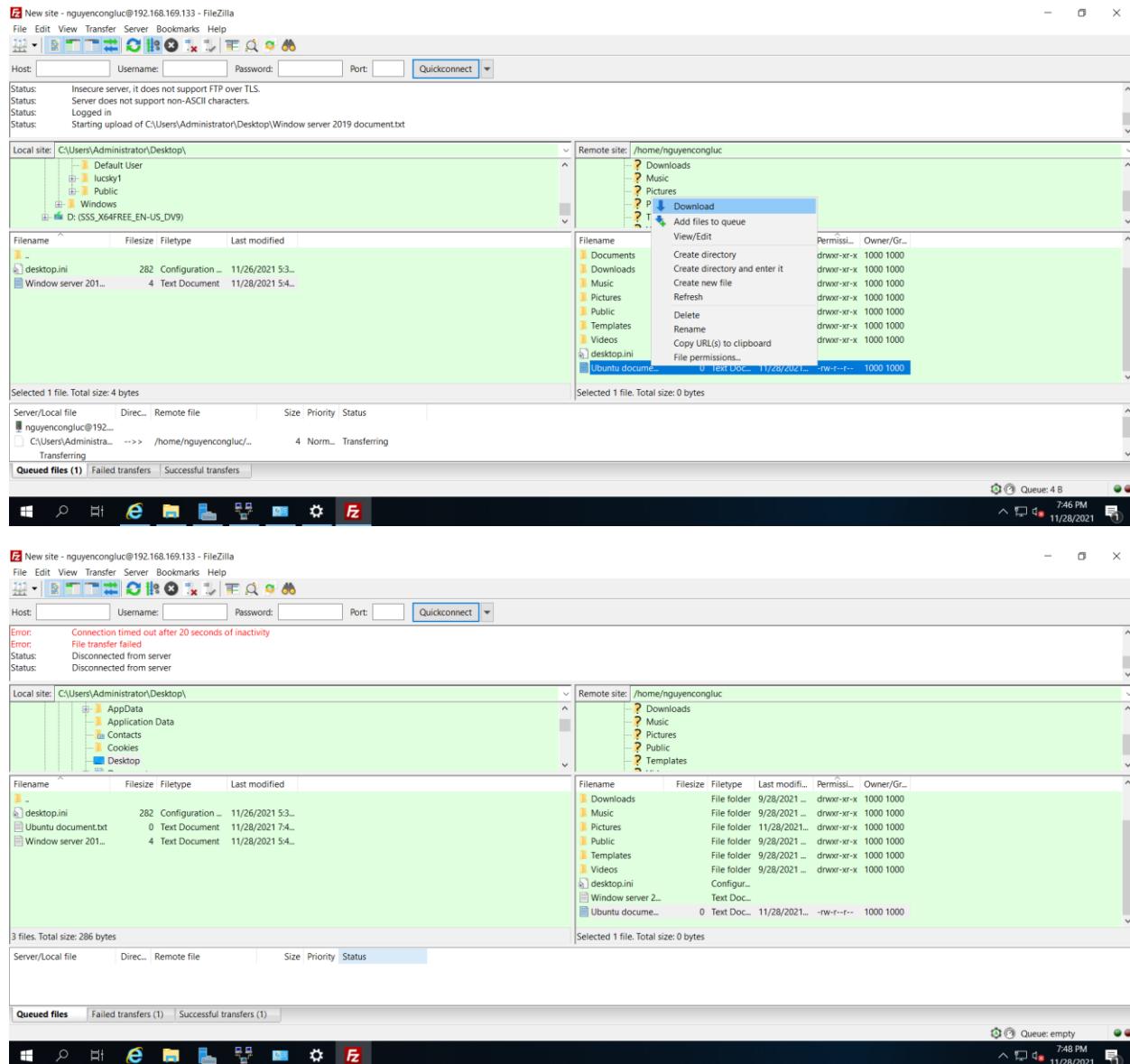


Thao tác cơ bản về: upload file, download

- Upload file



- Download file



2.2. Dịch vụ Quản trị từ xa: Remote Desktop Connection đến Server Ubuntu

- Cài đặt dịch vụ Remote desktop trên Ubuntu. (có phân quyền cho tài khoản Admin, user) - Kết nối VPN. - Sử dụng Remote desktop để kết nối.

B1: Tải về và cài đặt XRDP

```
nguyencongluc@infosec:~$ sudo apt install xrdp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  xorgxrdp
Suggested packages:
  guacamole xrdp-pulseaudio-installer
The following NEW packages will be installed:
  xorgxrdp xrdp
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 488 kB of archives.
After this operation, 3.212 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 xrdp amd64 0.9.12-1 [428 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 xorgxrdp amd64 1:0.2.12-1 [59,9 kB]
Fetched 488 kB in 0s (1.156 kB/s)
Selecting previously unselected package xrdp.
```

```
nguyencongluc@infosec:~$ sudo systemctl enable --now xrdp
Synchronizing state of xrdp.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable xrdp
```

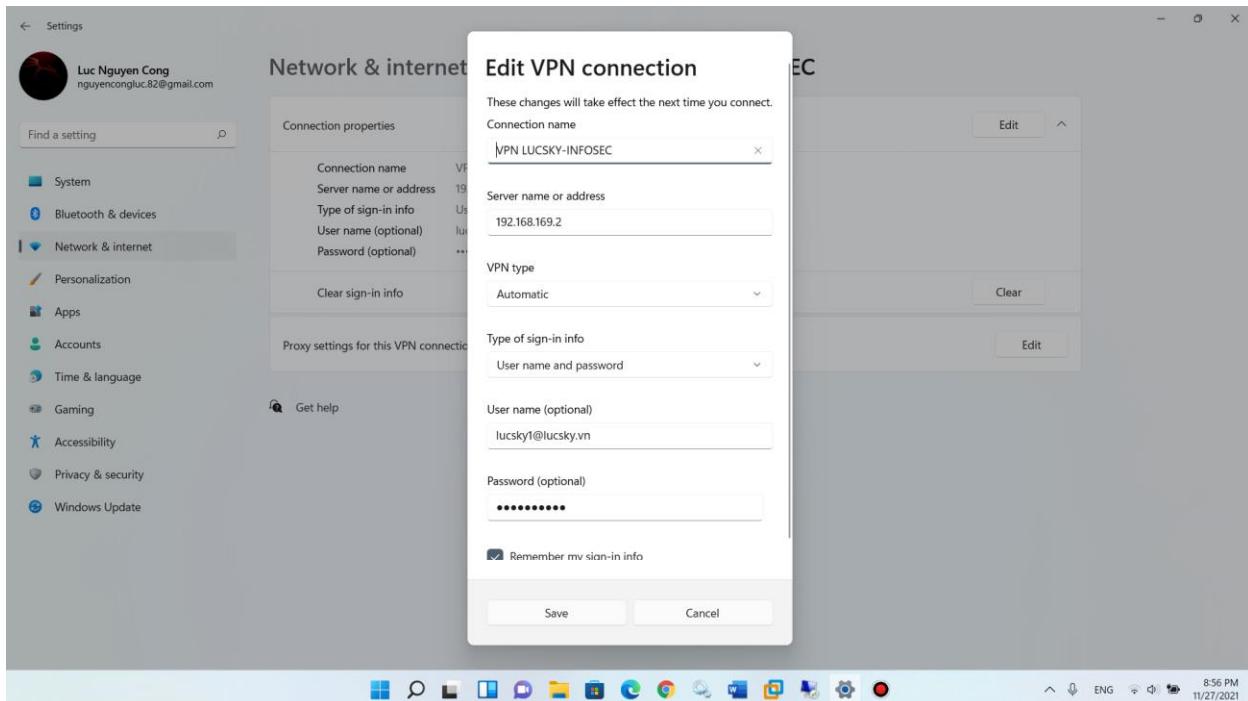
B2: Cho phép cổng RDP trong Tường lửa

```
nguyencongluc@infosec:~$ sudo ufw allow from any to any port 3389 proto tcp
Rule added
Rule added (v6)
nguyencongluc@infosec:~$ sudo ufw status
Status: active

To                         Action      From
--                         -----      ---
21/tcp                      ALLOW       Anywhere
40000:50000/tcp             ALLOW       Anywhere
990/tcp                     ALLOW       Anywhere
OpenSSH                      ALLOW       Anywhere
3389/tcp                    ALLOW       Anywhere
21/tcp (v6)                 ALLOW       Anywhere (v6)
40000:50000/tcp (v6)        ALLOW       Anywhere (v6)
990/tcp (v6)                ALLOW       Anywhere (v6)
OpenSSH (v6)                 ALLOW       Anywhere (v6)
3389/tcp (v6)               ALLOW       Anywhere (v6)

nguyencongluc@infosec:~$
```

B3: Kết nối VPN từ máy thật(window 11 pro) vào Window server 2019

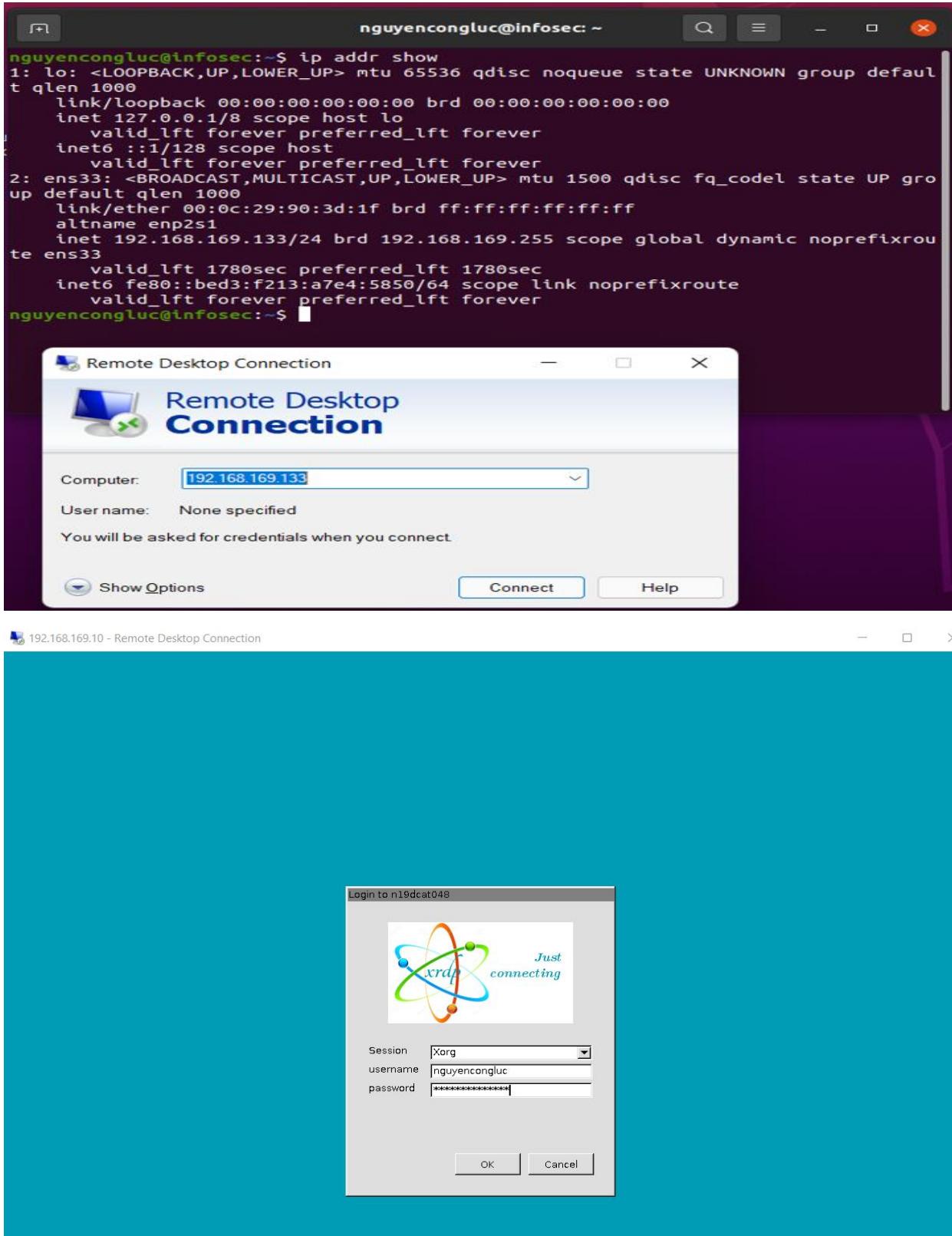


The screenshot shows the 'Routing and Remote Access' management console. The left navigation pane shows 'WIN-P3B6LLGD3E1 (local)' expanded, with 'Remote Access Clients (1)' selected. The main pane displays a table titled 'Remote Access Clients (1)' with one entry:

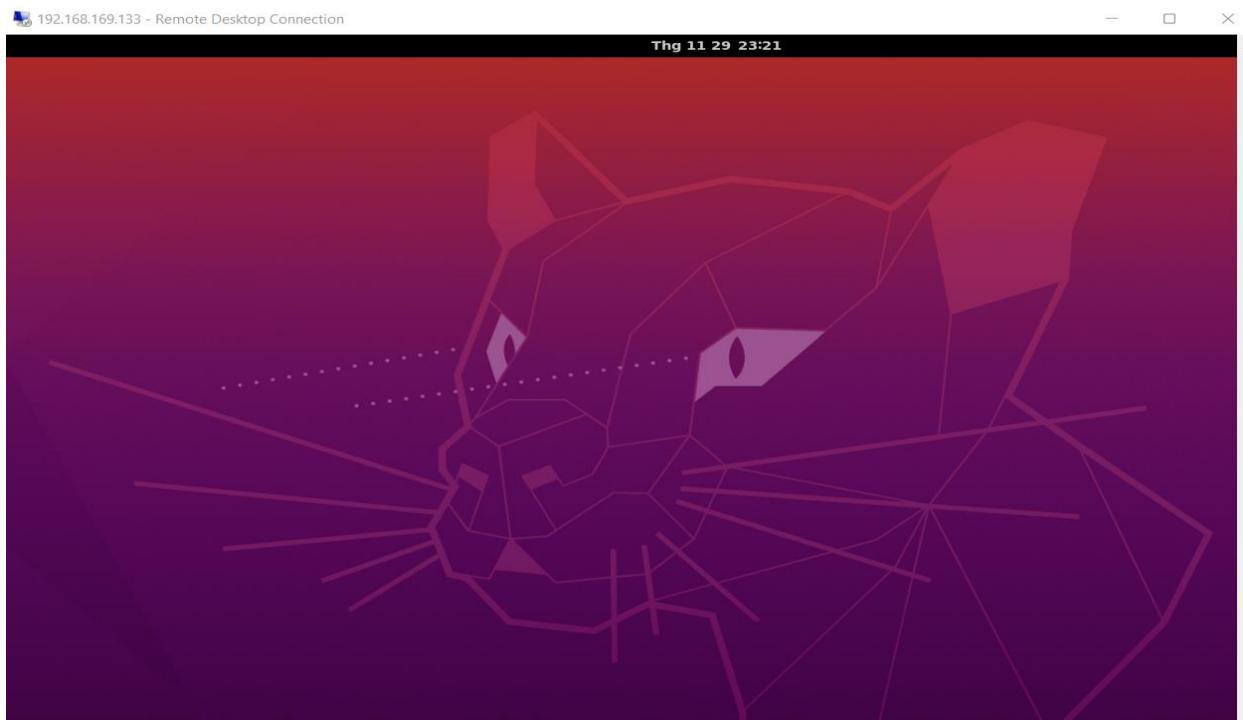
User Name	Duration	Number of Ports	Status
LUCSKY\lucsk...	00:00:16	1	Not NAP-ca...

At the bottom, a 'VPN connections' section shows 'VPN LUCSKY-INFOSEC Connected' with a 'Disconnect' button.

B4: Remote desktop từ máy thật (window 11 pro) vào Ubuntu server



Kết nối thành công



2.3. Dịch vụ Phân quyền User trong FTP Server

a. Cài đặt VSFTPD:

- Cài đặt gói VSFTPD: yum install vsftpd

```

root@n19dcat048-centos-domain:~ - □
File Edit View Search Terminal Help
[nguyencongluc@n19dcat048-centos-domain ~]$ sudo -i
[sudo] password for nguyencongluc:
[root@n19dcat048-centos-domain ~]# yum install vsftpd
Loaded plugins: fastestmirror, langpacks
Determining fastest mirrors
 * base: mirror.es.its.nyu.edu
 * extras: mirrors.oit.uci.edu
 * updates: centos.mirror.constant.com
base                                         | 3.6 kB     00:00
(1/2): base/7/x86_64/group_gz             | 153 kB    00:02
(2/2): base/7/x86_64/primary_db           | 6.1 MB    00:04
updates/7/x86_64/primary_db                | 12 MB     00:05
Resolving Dependencies
--> Running transaction check
---> Package vsftpd.x86_64 0:3.0.2-29.el7_9 will be installed
---> Finished Dependency Resolution

Dependencies Resolved
=====
Package          Arch      Version       Repository      Size
=====
Installing:
=====

```

```

root@n19dcat048-centos-domain:~ - □ ×
File Edit View Search Terminal Help
pm: Header V3 RSA/SHA256 Signature, key ID f4a80eb5: NOKEY
Public key for vsftpd-3.0.2-29.el7_9.x86_64.rpm is not installed
vsftpd-3.0.2-29.el7_9.x86_64.rpm                                | 173 kB   00:01
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
  Userid      : "CentOS-7 Key (Centos 7 Official Signing Key) <security@centos.org>"
  Fingerprint: 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a8 0eb5
  Package      : centos-release-7-9.2009.0.el7.centos.x86_64 (@anaconda)
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]: y
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : vsftpd-3.0.2-29.el7_9.x86_64                               1/1
  Verifying   : vsftpd-3.0.2-29.el7_9.x86_64                               1/1

Installed:
  vsftpd.x86_64 0:3.0.2-29.el7_9

Complete!
[root@n19dcat048-centos-domain ~]# █

```

- Copy file cấu hình để backups: /etc/vsftpd/vsftpd.conf

cp /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.example

b. Cấu hình FTP Server

- Chính sửa file cấu hình: vi /etc/vsftpd/vsftpd.conf

```
# không cho user mặc danh truy cập ftp server
anonymous_enable=NO

# sử dụng local user
local_enable=YES

# cho phép local user upload, delete file
write_enable=YES

# chroot và tạo 1 file /etc/vsftpd/chroot_list chứa danh sách các local user không bị giới
hạn bởi chroot

chroot_local_user=YES

allow_writeable_chroot=YES

chroot_list_enable=YES

chroot_list_file=/etc/vsftpd/chroot_list

# Ta chỉ sử dụng IPv4

listen=YES

# Không sử dụng IPv6

listen_ipv6=NO

# Chỉ cho các user có trong file /etc/vsftpd/user_list được truy cập FTP server

userlist_deny=NO

userlist_enable=YES

userlist_file=/etc/vsftpd/user_list

# Thư mục home của FTP Server

local_root=/var/ftp/

# Sử dụng thời gian của hệ thống

use_localtime=YES
```

```
root@n19dcat048-centos-domain:~ - □ ×
File Edit View Search Terminal Help
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
# When SELinux is enforcing check for SE bool ftp_home_dir
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
-- INSERT --
```

Nhấn esc và ctrl + z + z để lưu lại và thoát ra

-Khởi động vsftpd :

```
[root@n19dcat048-centos-domain ~]# systemctl start vsftpd
[root@n19dcat048-centos-domain ~]# systemctl enable vsftpd
Created symlink from /etc/systemd/system/multi-user.target.wants/vsftpd.service
to /usr/lib/systemd/system/vsftpd.service.
[root@n19dcat048-centos-domain ~]# █
```

-Cấu hình tường lửa:

```
root@n19dcat048-centos-domain:~ - □ ×
File Edit View Search Terminal Help
[root@n19dcat048-centos-domain ~]# firewall-cmd --permanent --add-port=21/tcp
success
[root@n19dcat048-centos-domain ~]# firewall-cmd --permanent --add-service=ftp
success
[root@n19dcat048-centos-domain ~]# firewall-cmd --reload
success
[root@n19dcat048-centos-domain ~]# █
```

- SELinux:

```
[root@n19dcat048-centos-domain ~]# setsebool -P ftpd_full_access on
[root@n19dcat048-centos-domain ~]# █
```

c. Tạo các user và phân quyền

-Tạo các user và group

Tạo 3 user: user1, user2, user3 và thay đổi Home directory của chúng như sau:

```
root@n19dcat048-centos-domain:~ - □ ×
File Edit View Search Terminal Help
[root@n19dcat048-centos-domain ~]# useradd -d /var/ftp/user1 user1
[root@n19dcat048-centos-domain ~]# useradd -d /var/ftp/user2 user2
[root@n19dcat048-centos-domain ~]# useradd -d /var/ftp/user3 user3
[root@n19dcat048-centos-domain ~]#
```

Đặt mật khẩu cho các user vừa tạo

```
[root@n19dcat048-centos-domain ~]# passwd user1
Changing password for user user1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@n19dcat048-centos-domain ~]# passwd user2
Changing password for user user2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@n19dcat048-centos-domain ~]# passwd user3
Changing password for user user3.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@n19dcat048-centos-domain ~]#
```

Tạo 2 group

- o ftp_basic : user có quyền bình thường đối với thư mục của mình và thư mục dùng chung. Dùng cho user1 và user2.
- o ftp_onlyread : user chỉ có quyền đọc. Dùng cho user3.

```
[root@n19dcat048-centos-domain ~]# groupadd ftp_basic
[root@n19dcat048-centos-domain ~]# groupadd ftp_onlyread
[root@n19dcat048-centos-domain ~]#
```

Thêm các user vào 2 group vừa tạo:

```
[root@n19dcat048-centos-domain ~]# usermod -g ftp_onlyread user3
[root@n19dcat048-centos-domain ~]# usermod -g ftp_basic user2
[root@n19dcat048-centos-domain ~]# usermod -g ftp_basic user1
```

d. Cấp quyền truy cập và phân quyền các user:

Cấp quyền truy cập FTP server cho các user vừa tạo bằng cách thêm vào file /etc/vsftpd/user_list, mỗi user trên một dòng và lưu lại.

Thêm vào danh sách không bị chroot giới hạn

```
[root@n19dcat048-centos-domain ~]# vi /etc/vsftpd/user_list
```

```
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
user1
user2
user3■
```

Tạo 1 thư mục dùng chung cho *user1* và *user2* tên là /user12:

```
[root@n19dcat048-centos-domain ~]# mkdir /var/ftp/user12
```

Thay đổi quyền sở hữu thư mục:

```
[root@n19dcat048-centos-domain ~]# chown -R user1:ftp_basic /var/ftp/user1
[root@n19dcat048-centos-domain ~]# chown -R user2:ftp_basic /var/ftp/user2
[root@n19dcat048-centos-domain ~]# chown -R user3:ftp_onlyread /var/ftp/user3
[root@n19dcat048-centos-domain ~]# chown -R :ftp basic /var/ftp/user12
```

Thay đổi permission để kiểm soát truy cập của từng user đối với các thư mục



Quyền và permission của các user với các thư mục:

	/user1			/user2			/user3			/user12		
	đọc	ghi	thực thi	đọc	ghi	thực thi	đọc	ghi	thực thi	đọc	ghi	thực thi
user1	x	x	x							x	x	x
user2				x	x	x				x	x	x
user3	x			x			x			x		
Permission	705			705			550			775		

```
[root@n19dcat048-centos-domain ~]# chmod 705 /var/ftp/user1
[root@n19dcat048-centos-domain ~]# chmod 705 /var/ftp/user2
[root@n19dcat048-centos-domain ~]# chmod 550 /var/ftp/user3
[root@n19dcat048-centos-domain ~]# chmod 775 /var/ftp/user12
```

Như vậy ta đã phân quyền xong. Ta tiến hành restart lại dịch vụ vsftpd:

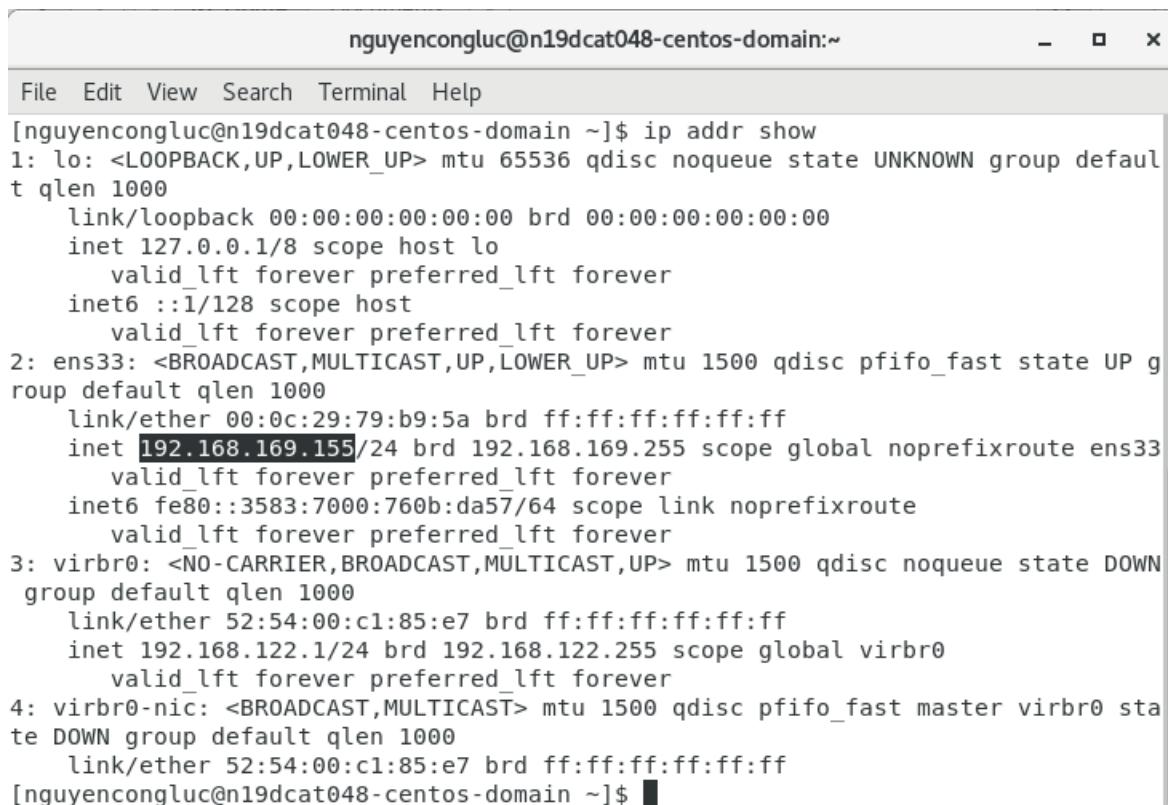
```
[root@n19dcat048-centos-domain ~]# systemctl restart vsftpd
```

d. Sử dụng FileZilla để truy cập FTP server kiểm tra phân quyền

****user1 và user2**

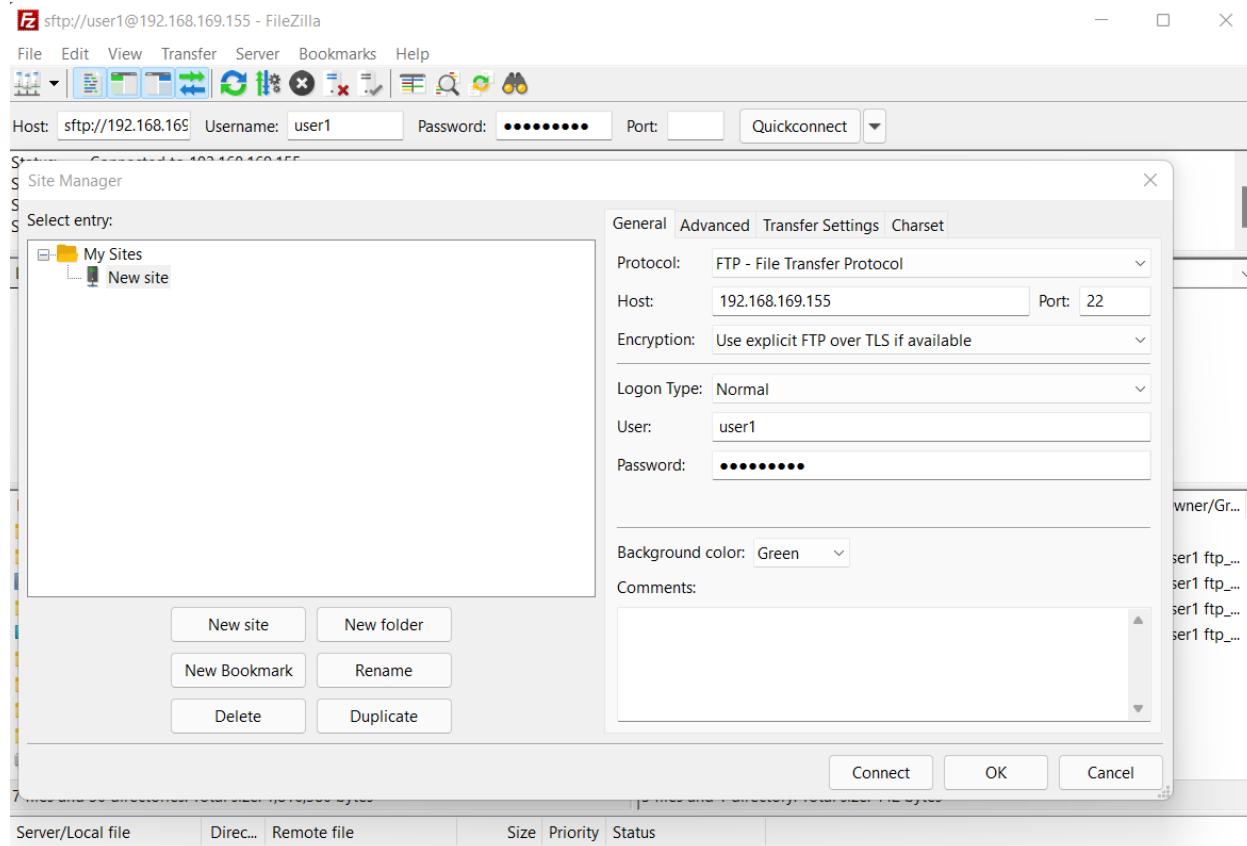
Ở đây, sẽ thử với user1. (user2 hoàn toàn tương tự)

Địa chỉ ip máy centos 7



The screenshot shows a terminal window titled "nguyencongluc@n19dcat048-centos-domain:~". The window contains the output of the "ip addr show" command. The output lists network interfaces (lo, ens33, virbr0, virbr0-nic) with their respective MAC addresses, broadcast addresses, and IP configurations. The "lo" interface has an IP of 127.0.0.1/8. The "ens33" interface has an IP of 192.168.169.155/24. The "virbr0" interface has an IP of 192.168.122.1/24. The "virbr0-nic" interface is a bridge interface with no specific IP listed.

```
nguyencongluc@n19dcat048-centos-domain:~
File Edit View Search Terminal Help
[nguyencongluc@n19dcat048-centos-domain ~]$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:79:b9:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.169.155/24 brd 192.168.169.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::3583:7000:760b:da57/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:c1:85:e7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:c1:85:e7 brd ff:ff:ff:ff:ff:ff
[nguyencongluc@n19dcat048-centos-domain ~]$
```



The screenshot shows the main FileZilla interface with two panes. The left pane shows the 'Local site' as 'D:\' with contents including Desktop, Documents, This PC, C: (Windows 11 Pro), and D:. The right pane shows the 'Remote site' as '/var/ftp' with contents including /, var, ftp, pub, user1, user2, and user3. Below the panes are two tables comparing files.

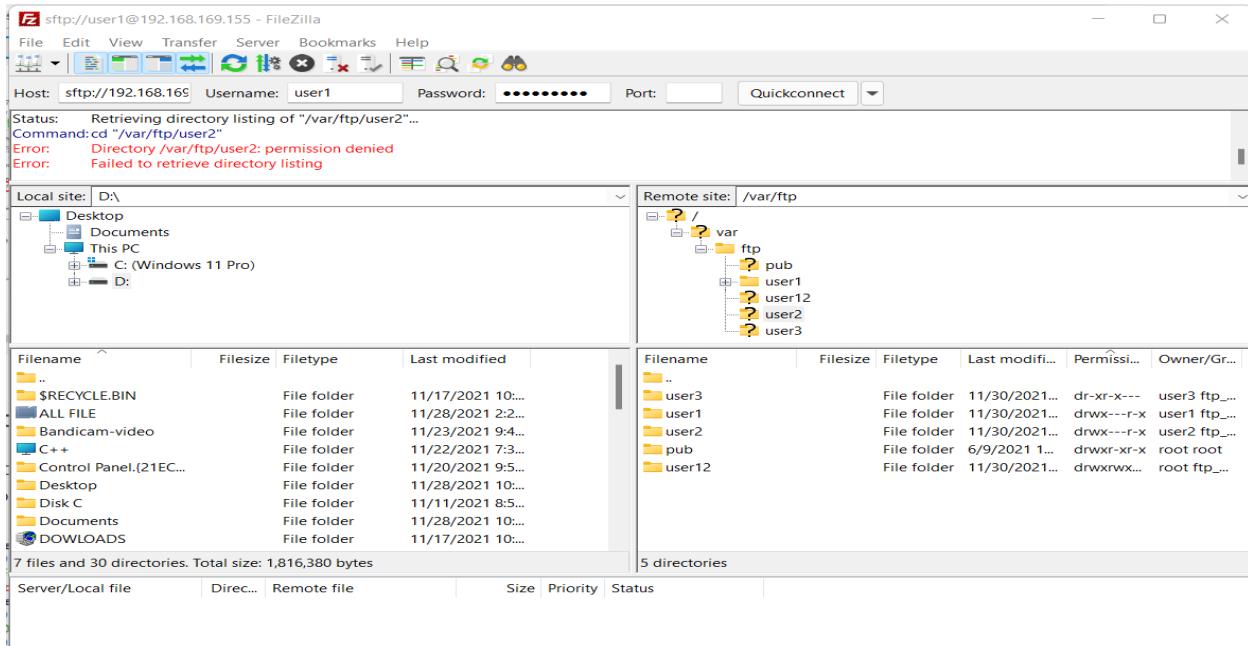
Local site	Remote site
D:\	/var/ftp
Desktop	/
Documents	var
This PC	ftp
C: (Windows 11 Pro)	pub
D:	user1
	user2
	user3

Filename	Filesize	Filetype	Last modified	Permiss...	Owner/Gr...
..					
\$RECYCLE.BIN		File folder	11/17/2021 10...		
ALL FILE		File folder	11/28/2021 2:2...		
Bandicam-video		File folder	11/23/2021 9:4...		
C ++		File folder	11/22/2021 7:3...		
Control Panel.(21EC...		File folder	11/20/2021 9:5...		
Desktop		File folder	11/28/2021 10...		
Disk C		File folder	11/11/2021 8:5...		
Documents		File folder	11/28/2021 10...		
DOWLOADS		File folder	11/17/2021 10...		

Filename	Filesize	Filetype	Last modified	Permiss...	Owner/Gr...
..					
user3		File folder	11/30/2021...	dr-xr-x---	user3 ftp_...
user1		File folder	11/30/2021...	drwx---r-x	user1 ftp_...
user2		File folder	11/30/2021...	drwx---r-x	user2 ftp_...
pub		File folder	6/9/2021 1...	drwxr-xr-x	root root
user12		File folder	11/30/2021...	drwxrwx...	root ftp_...

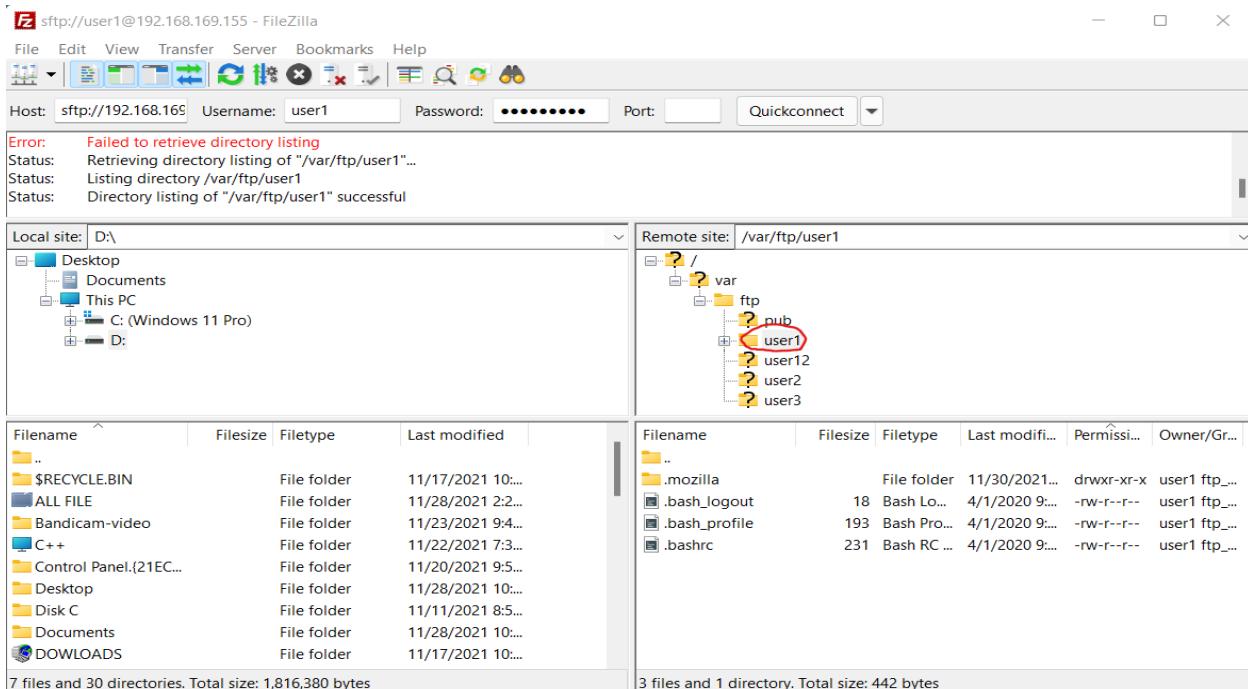
*Truy cập vào các thư mục không thuộc quyền sở hữu

Khi thử truy cập vào các thư mục không thuộc quyền sở hữu ví dụ ở đây thử truy cập vào 2 thư mục là /user2 và /user3 sẽ không thành công và hiện thông báo lỗi như hình:

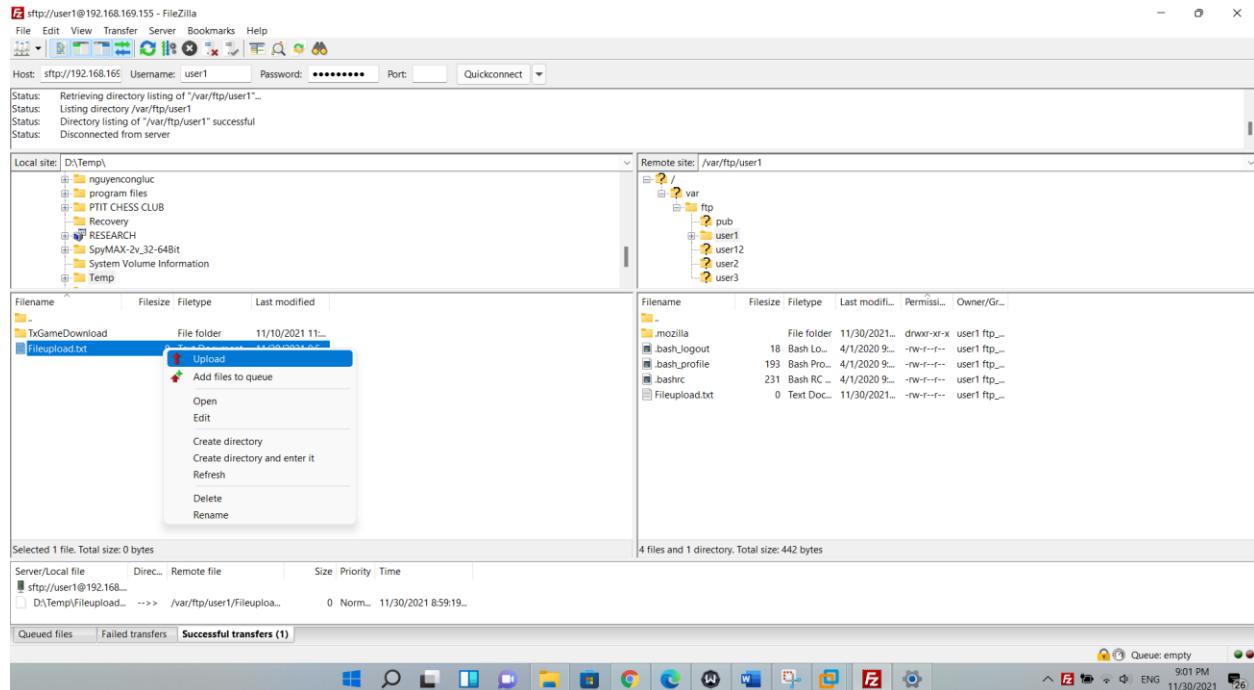


*Truy cập vào thư mục cá nhân

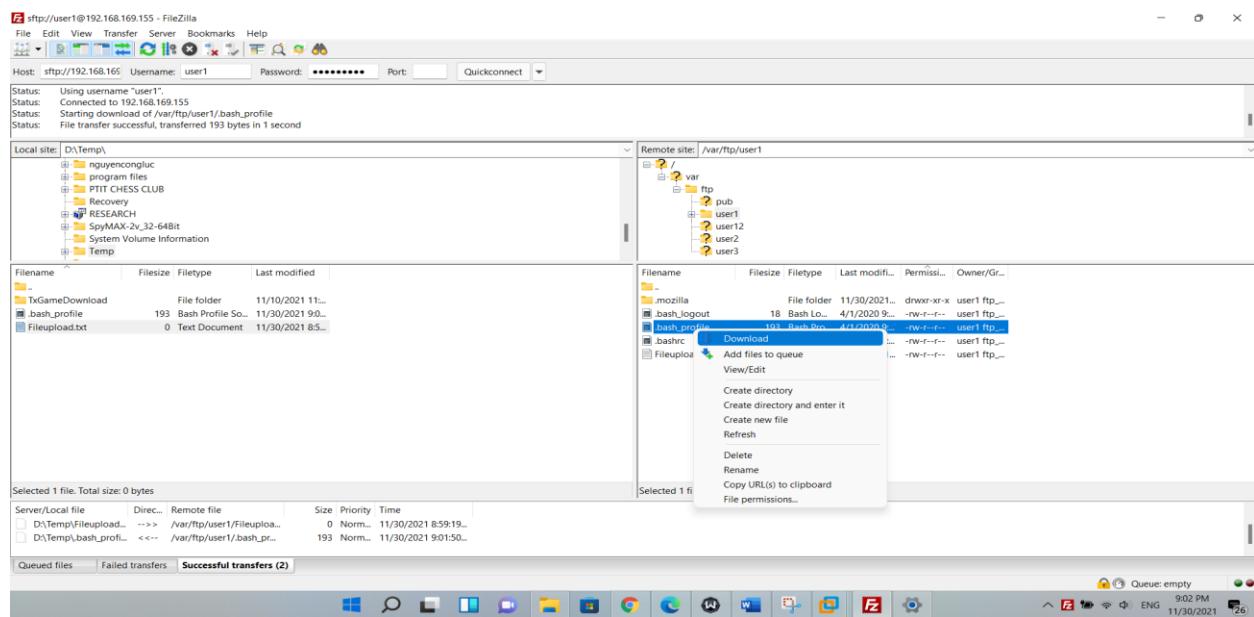
Nếu truy cập vào thư mục cá nhân là /user1: ta sẽ thấy các nội dung trong thư mục /user1



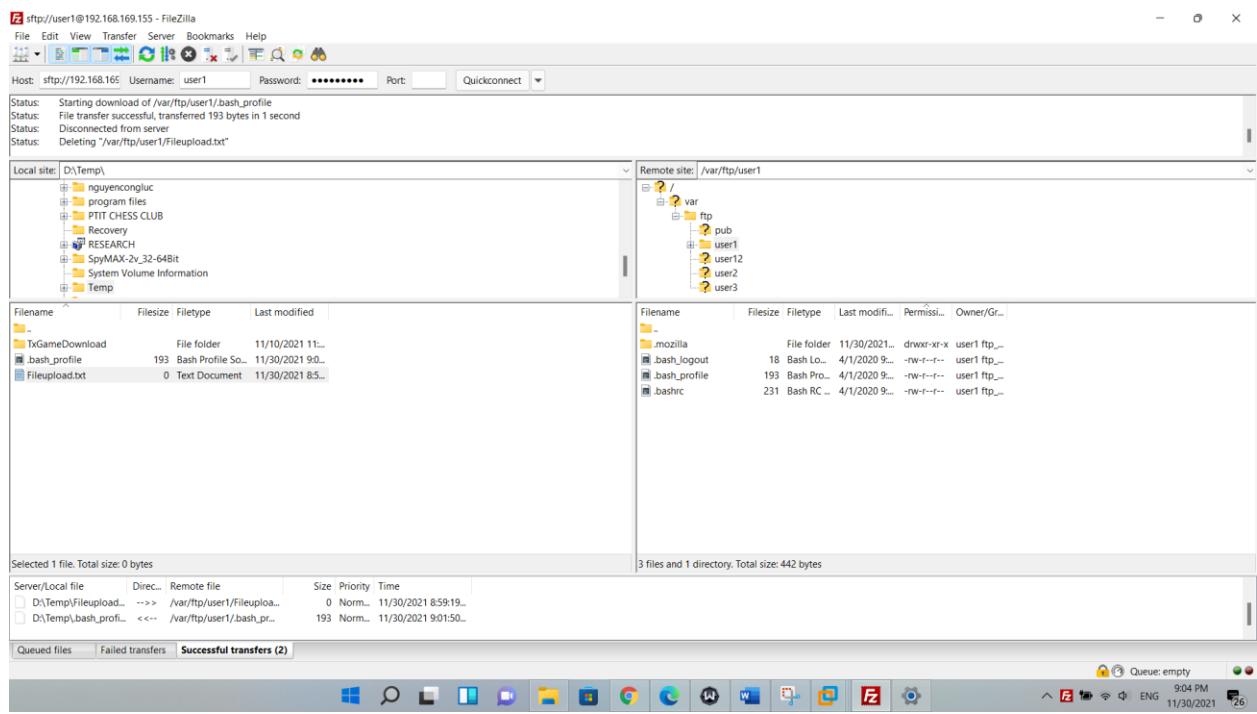
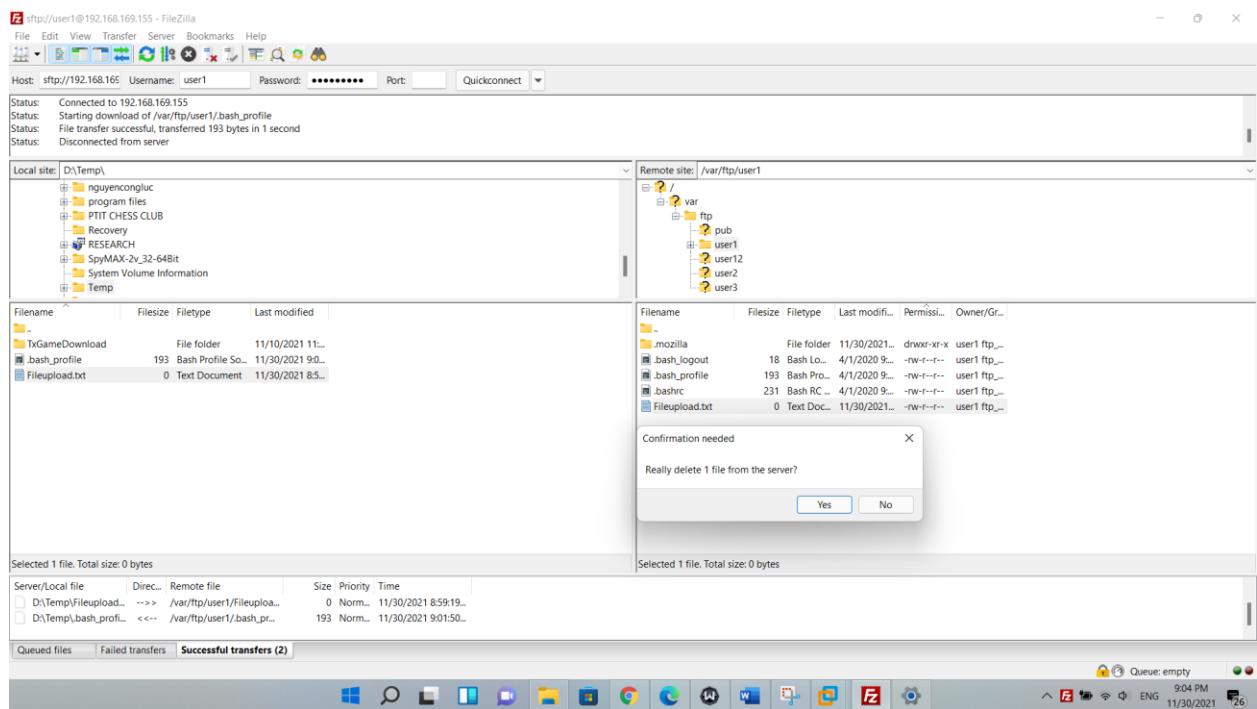
- **Upload file:** Ta sẽ upload file *fileupload.txt* từ local lên thư mục /user1 của FTP server. Ta sẽ thấy thông báo thành công và file hiển thị trên FTP server.



- **Download file:** Ta sẽ download file *.bash_profile* về local. Ta sẽ thực hiện thành công việc download như hình

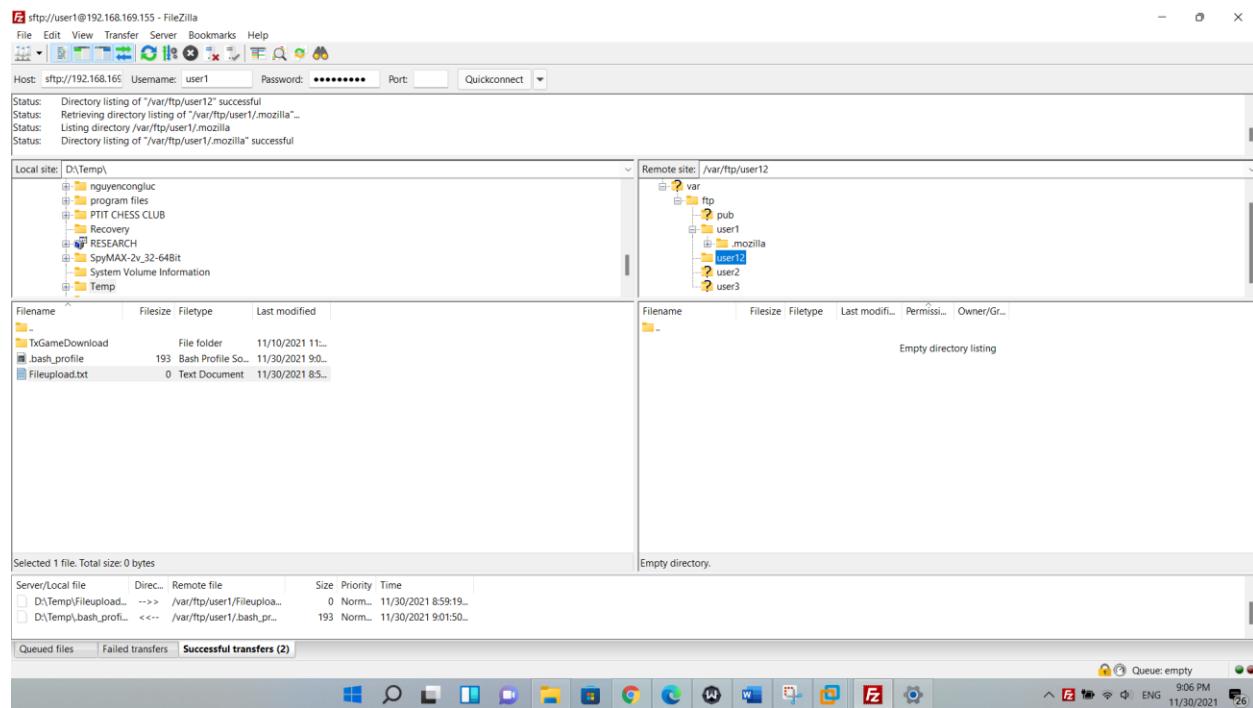


- Xóa file trên FTP server: xóa file *fileupload.txt*

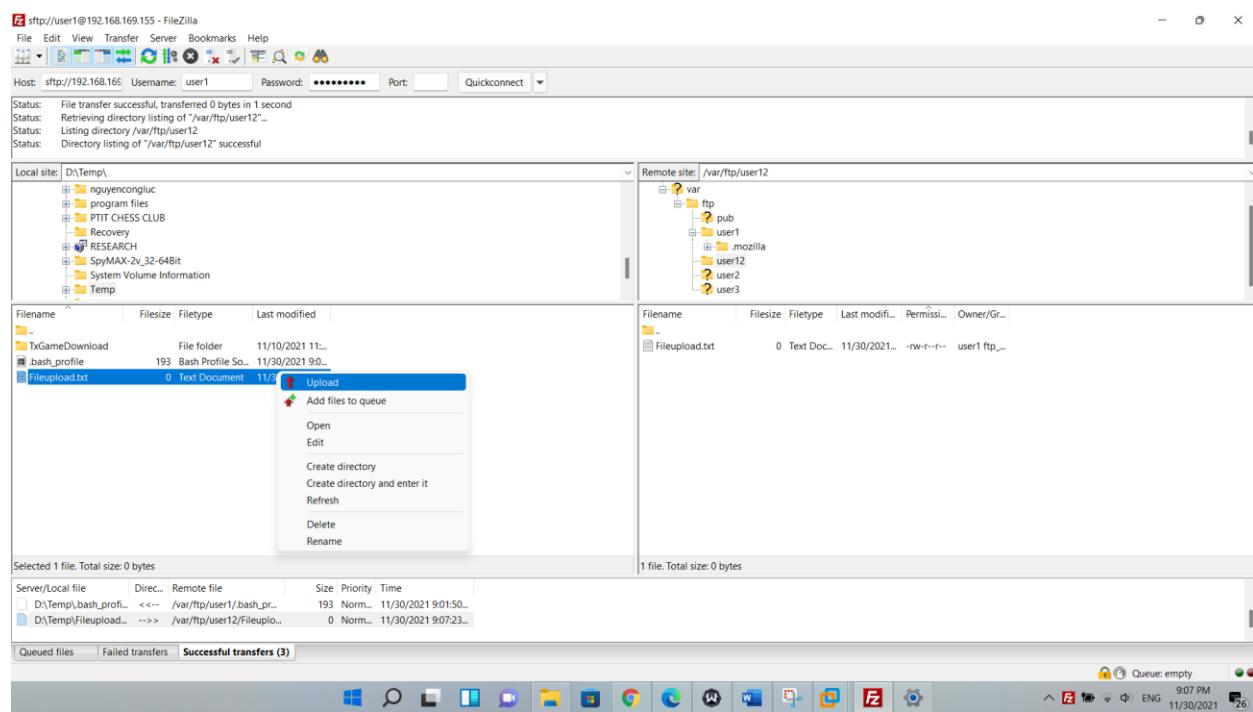


*Truy cập thư mục chung /user12

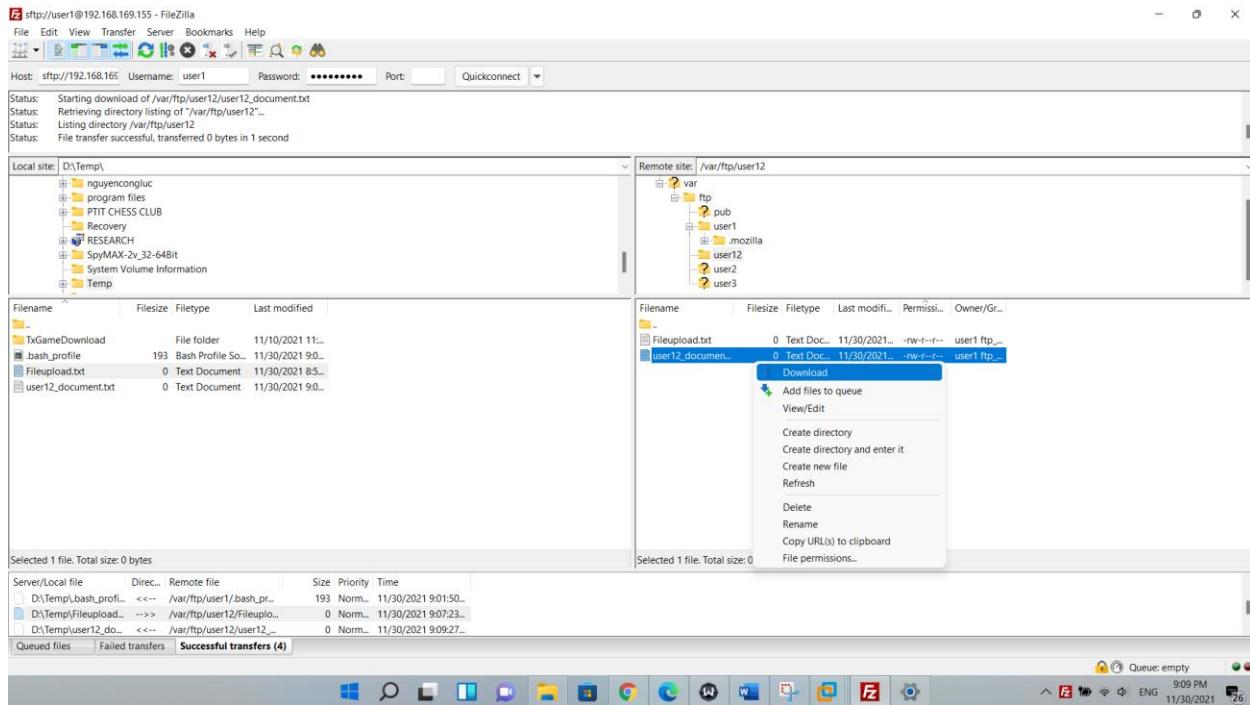
- Truy cập thư mục: /user12



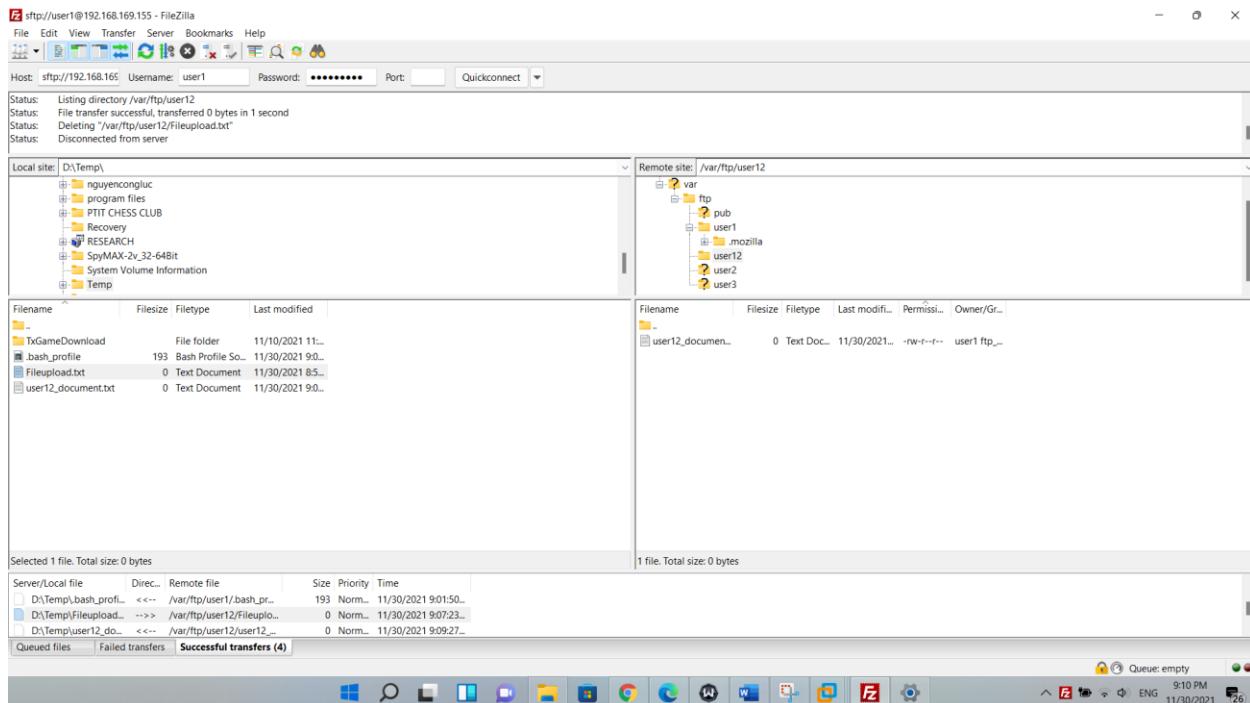
- Upload file:



- Download:



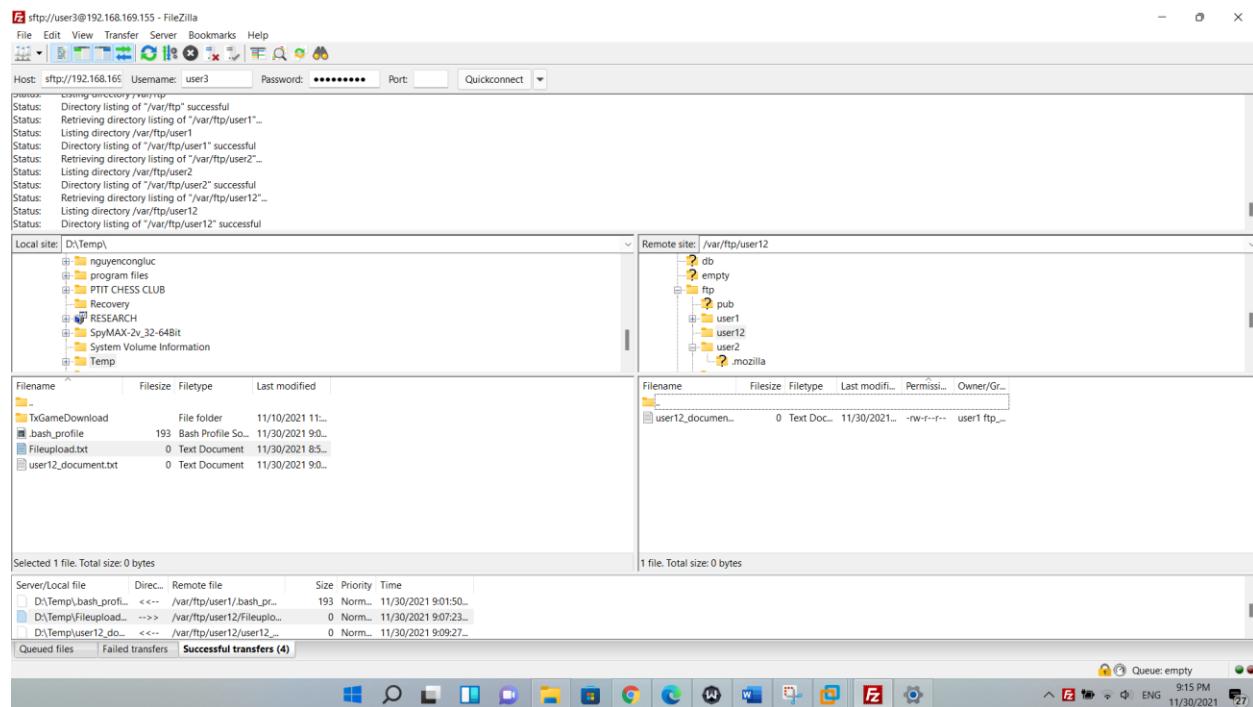
- Xóa file: xóa file *fileupload.txt*



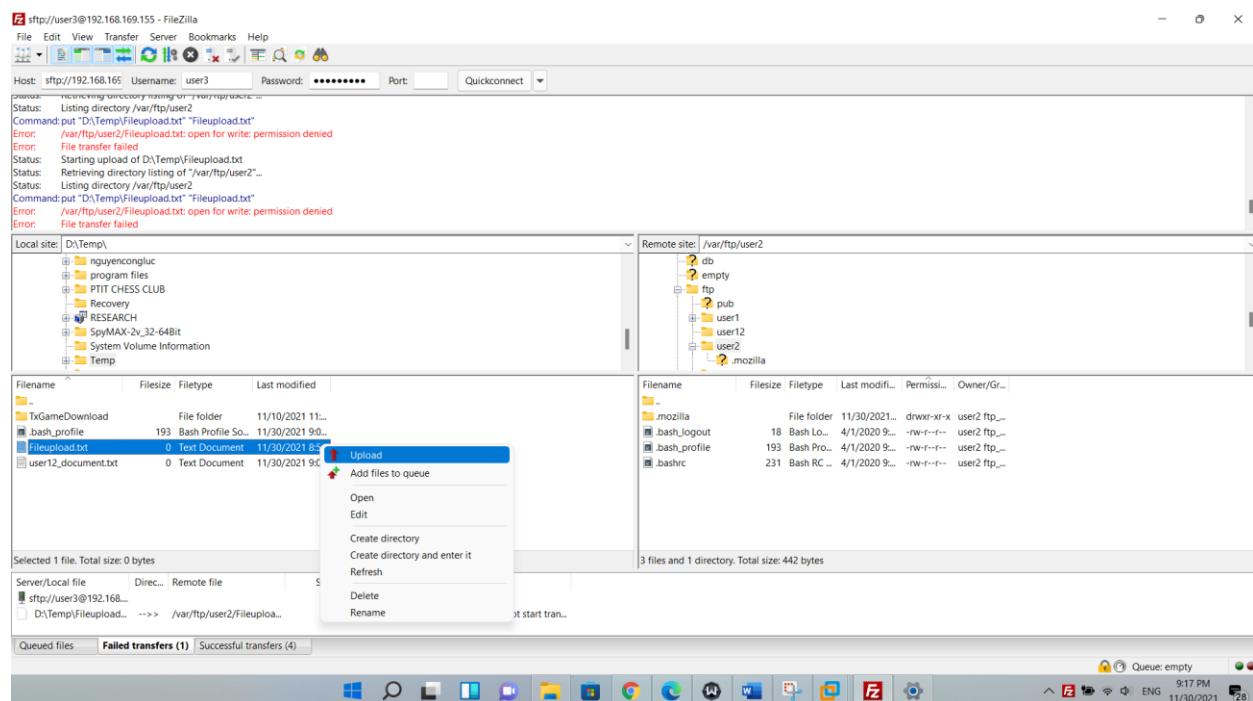
**user3

user3 có thể truy cập tất cả các thư mục trên FTP server, tuy nhiên nó chỉ có thể xem nội dung và download mà không thể chỉnh sửa nội dung trên FTP Server

- Truy cập các thư mục trên FTP server

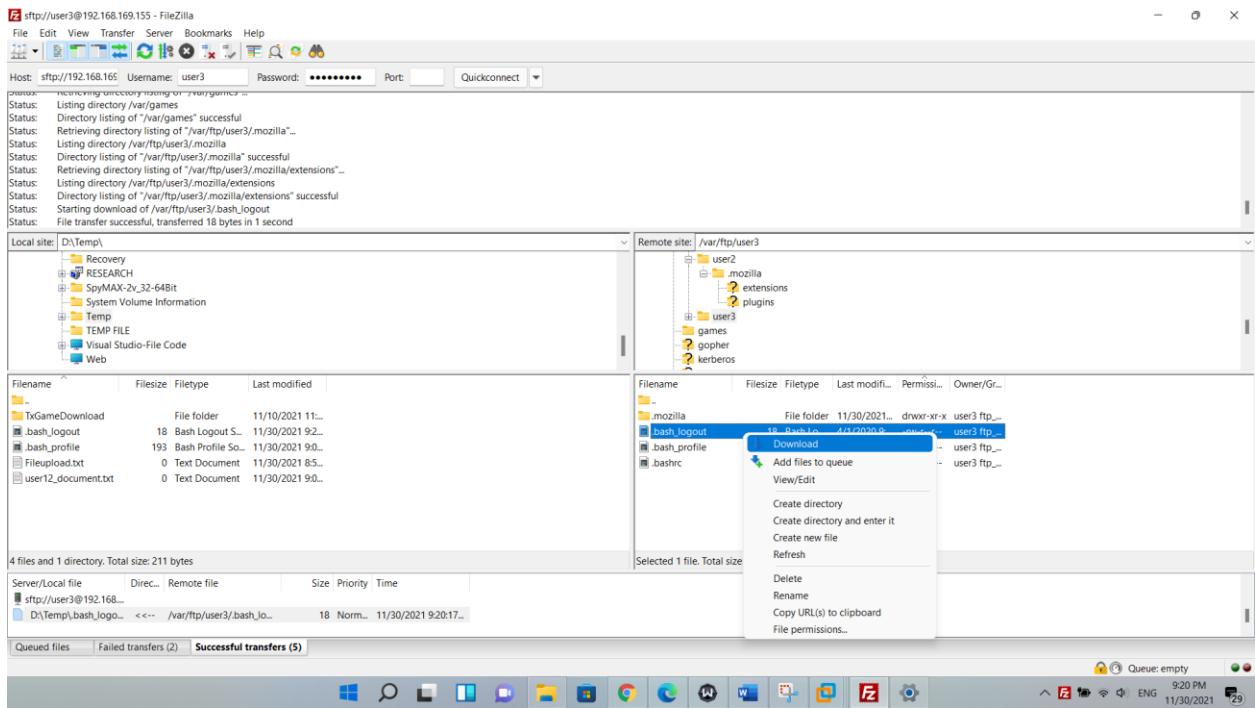


- Upload file: không upload thành công lên Server

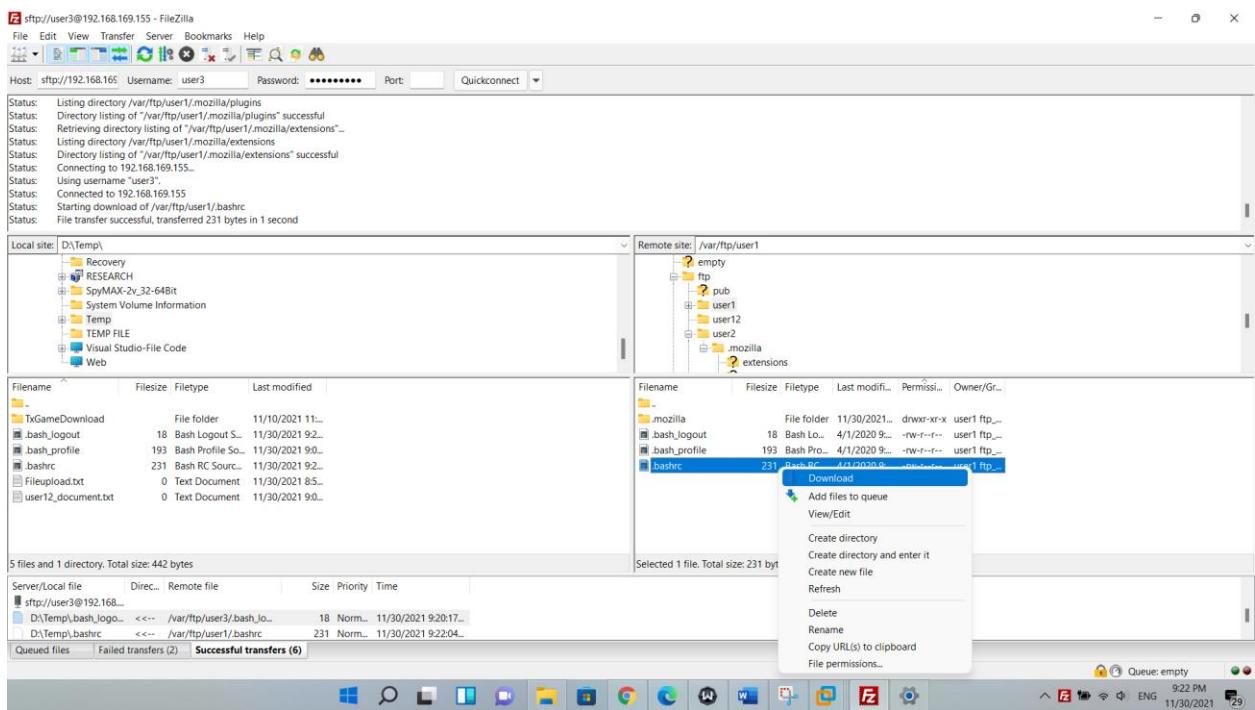


- **Download file:**

Trên thư mục /user3: Dowload file .bash_logout thành công

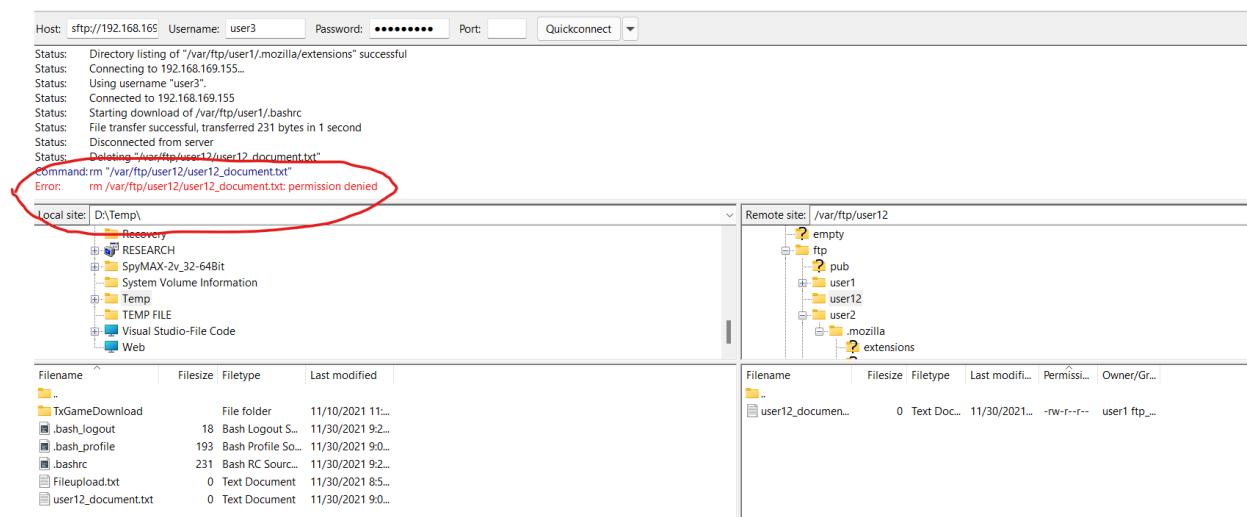
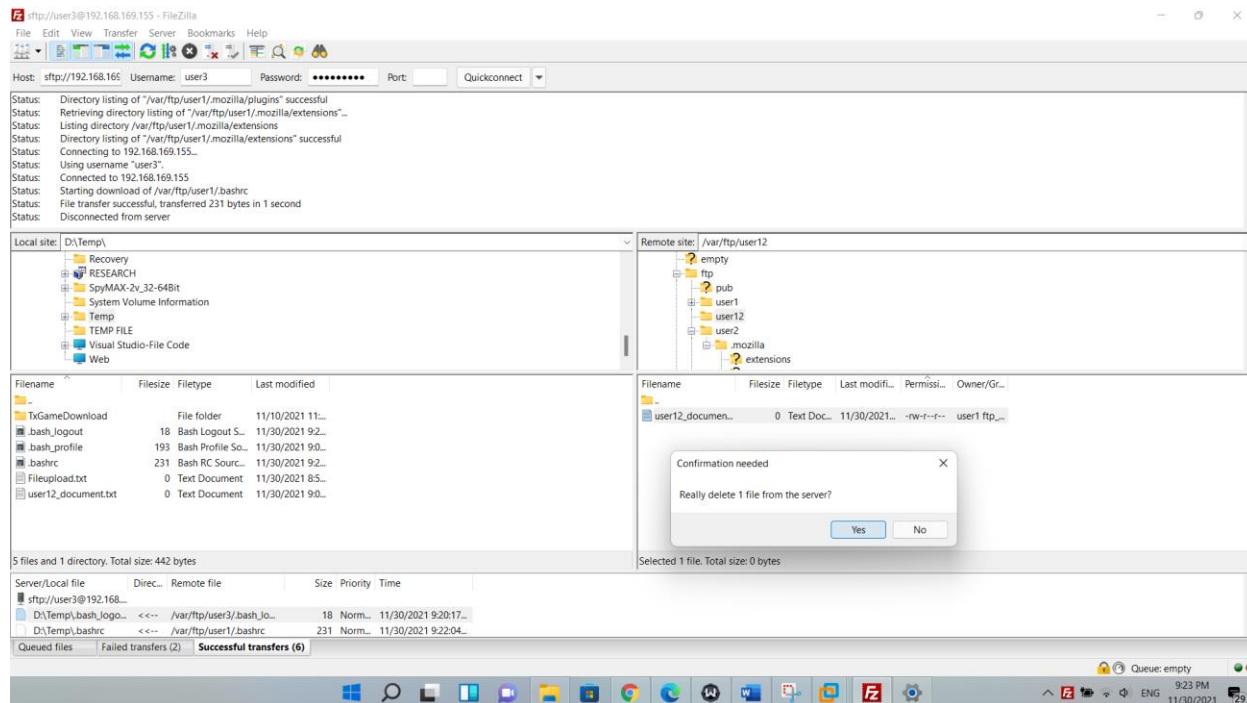


Trên các thư mục khác: Dowload file .bashrc từ folder user1 thành công



- **Xóa file:** không thể thực hiện

Trên các thư mục khác:



Trên thư mục /user3

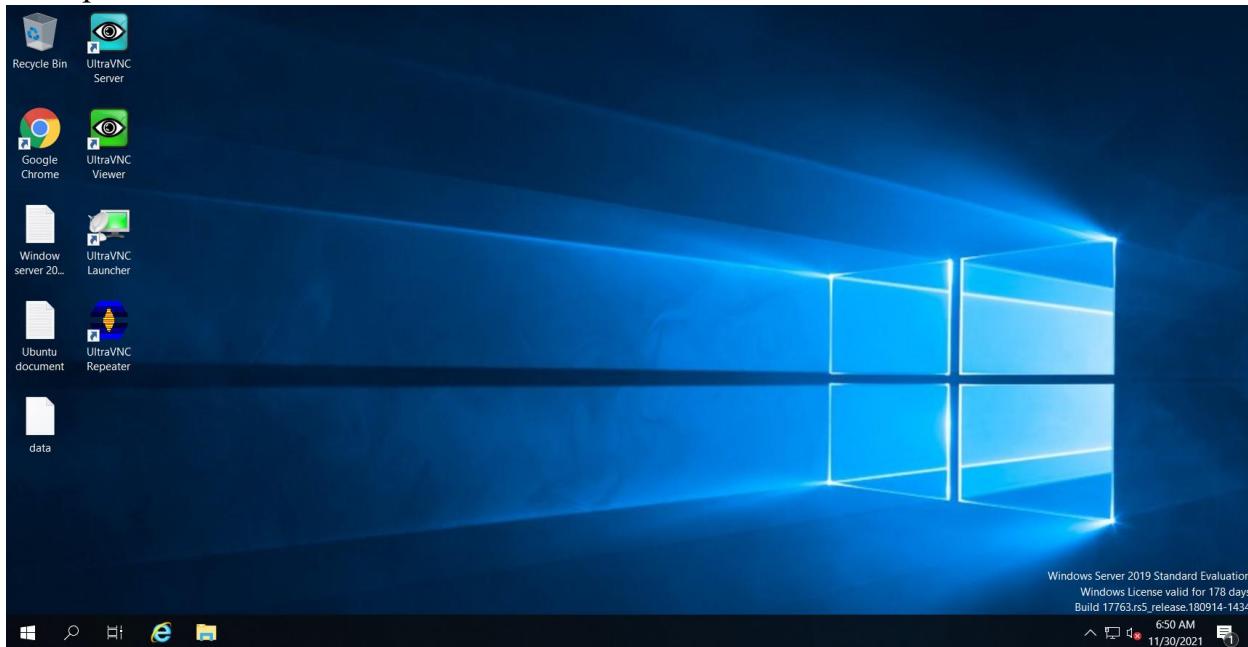
Host: sftp://192.168.169.155 Username: user3 Password: Port: Quickconnect

Status: Connected to 192.168.169.155
Status: Starting download of /var/ftp/user1/.bashrc
Status: File transfer successful, transferred 231 bytes in 1 second
Status: Disconnected from server
Status: Deleting "/var/ftp/user12/user12_document.txt"
Command: rm "/var/ftp/user12/user12_document.txt": permission denied
Error: rm "/var/ftp/user12/user12_document.txt": permission denied
Status: Deleting "/var/ftp/user3/.bashrc"
Command: rm "/var/ftp/user3/.bashrc"
Error: rm "/var/ftp/user3/.bashrc": permission denied

Local site: D:\Temp		Remote site: /var/ftp/user3	
Filename	Filesize	Filetype	Last modified
..		File folder	11/10/2021 11:...
TxGameDownload		File folder	11/10/2021 11:...
.bash_logout	18	Bash Logout S...	11/30/2021 9:2...
.bash_profile	193	Bash Profile So...	11/30/2021 9:0...
.bashrc	231	Bash RC Sourc...	11/30/2021 9:2...
Fileupload.txt	0	Text Document	11/30/2021 8:5...
user12_document.txt	0	Text Document	11/30/2021 9:0...

2.4. Dịch vụ Quản trị từ xa:

- Cài phần mềm: UltraVNC Viewer



Bước: 1 Đảm bảo rằng các Gói Máy tính để bàn đã được cài đặt Để thiết lập máy chủ VNC, trước tiên chúng tôi đảm bảo rằng Máy tính để bàn đã được cài đặt, trong trường hợp của tôi, tôi đang sử dụng Máy tính để bàn Gnome. Nếu Gnome Desktop chưa được cài đặt trên máy Linux của bạn thì hãy sử dụng lệnh dưới đây để cài đặt

```
[root@n19dcat048-centos-domain ~]# yum groupinstall "GNOME Desktop"
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.es.its.nyu.edu
 * extras: mirror.clarkson.edu
 * updates: mirror.es.its.nyu.edu
```

```
[root@n19dcat048-centos-domain ~]# yum install tigervnc-server
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.es.its.nyu.edu
 * extras: mirror.clarkson.edu
 * updates: mirror.es.its.nyu.edu
base                                         | 3.6 kB     00:00
extras                                        | 2.9 kB     00:00
updates                                       | 2.9 kB     00:00
Resolving Dependencies
--> Running transaction check
---> Package tigervnc-server.x86_64 0:1.8.0-22.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package          Arch      Version       Repository    Size
=====
Installing:
tigervnc-server x86_64  1.8.0-22.el7   updates       211 k

Transaction Summary
```

Bước: 2 Cài đặt Tigervnc và Gói phụ thuộc khác

```
[root@n19dcat048-centos-domain ~]# yum install tigervnc-server xorg-x11-fonts-Type1
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.es.its.nyu.edu
 * extras: mirror.clarkson.edu
 * updates: mirror.es.its.nyu.edu
Package tigervnc-server-1.8.0-22.el7.x86_64 already installed and latest version
Package xorg-x11-fonts-Type1-7.5-9.el7.noarch already installed and latest version
Nothing to do
```

Bước: 3 Thiết lập tệp cấu hình máy chủ VNC. Sao chép tệp cấu hình VNC

“/lib/systemd/system/vncserver@.service” to the “/etc/systemd/system/vncserver@:.service”. Trong khi sao chép tệp cấu hình VNC, chúng ta có thể đề cập đến số cổng mà chúng ta muốn dịch vụ VNC lắng

nghe. Trong trường hợp của tôi, tôi đang sử dụng cổng 3, có nghĩa là VNC sẽ lắng nghe trên “5903”. Vì vậy, trong khi kết nối với máy chủ VNC, chúng tôi có thể chỉ định số cổng là hoặc

```
[root@n19dcat048-centos-domain ~]# cp /lib/systemd/system/vncserver@.service /etc/systemd/system/vncserver@:3.service
```

Bước: 4 Cập nhật thông tin người dùng trong tệp cấu hình

```
[root@n19dcat048-centos-domain ~]# nano /etc/systemd/system/vncserver@:3.service
```

```
GNU nano 2.3.1      File: /etc/systemd/system/vncserver@:3.service      Modified

# See the ssh man page for details on port forwarding)
#
# You can then point a VNC client on hostA at vncdisplay N of localhost and with
# the help of ssh, you end up seeing what hostB makes available on port 590M
#
# Use "-nolisten tcp" to prevent X connections to your VNC server via TCP.
#
# Use "-localhost" to prevent remote VNC clients connecting except when
# doing so through a secure tunnel. See the "-via" option in the
# `man vncviewer` manual page.

[Unit]
Description=Remote desktop service (VNC)
After=syslog.target network.target

[Service]
Type=simple

# Clean any existing files in /tmp/.X11-unix environment
ExecStartPre=/bin/sh -c '/usr/bin/vncserver -kill %i > /dev/null 2>&1 || :'
ExecStart=/sbin/runuser -l root -c "/usr/bin/vncserver %i"
PIDFile=/root/.vnc/%H%i.pid
ExecStop=/bin/sh -c '/usr/bin/vncserver -kill %i > /dev/null 2>&1 || :'

[Install]
WantedBy=multi-user.target
```

Trong trường hợp này, người dùng root(user n19dcat094 đang login) sẽ có thể điều khiển và quản lý phiên làm việc trên máy tính của mình bằng các ứng dụng khách VNC từ xa

Đặt Quy tắc tường lửa nếu tường lửa được bật trên hộp linux

```
[root@n19dcat048-centos-domain ~]# firewall-cmd --permanent --zone=public --add-port=5903/tcp
success
[root@n19dcat048-centos-domain ~]# firewall-cmd --reload
success
```

Bước: 5 Đặt mật khẩu VNC cho Người dùng.(Trường hợp này mình dùng user đang login)

Chuyển sang người dùng

```
[root@n19dcat048-centos-domain ~]# su -
Last login: Wed Dec  1 09:07:05 +07 2021 on pts/0
[root@n19dcat048-centos-domain ~]# vncserver

You will require a password to access your desktops.

Password:
Verify:
Would you like to enter a view-only password (y/n)? Y
Password:
Verify:

New 'n19dcat048-centos-domain:1 (root)' desktop is n19dcat048-centos-domain:1

Creating default startup script /root/.vnc/xstartup
Creating default config /root/.vnc/config
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/n19dcat048-centos-domain:1.log
```

Khởi động và Kích hoạt Dịch vụ VNC khi khởi động.

Chỉ thực thi các lệnh dưới đây với tư cách là người chủ.

```
[root@n19dcat048-centos-domain ~]# systemctl daemon-reload
[root@n19dcat048-centos-domain ~]# systemctl start vncserver@:3.service
[root@n19dcat048-centos-domain ~]# systemctl enable vncserver@:3.service
Created symlink from /etc/systemd/system/multi-user.target.wants/vncserver@:3.service to /etc/systemd/system/vncserver@:3.service.
[root@n19dcat048-centos-domain ~]# systemctl status vncserver@:3.service
● vncserver@:3.service - Remote desktop service (VNC)
  Loaded: loaded (/etc/systemd/system/vncserver@:3.service; enabled; vendor preset: disabled)
  Active: active (running) since Wed 2021-12-01 09:11:20 +07; 1min 51s ago
    Main PID: 8099 (Xvnc)
      CGroup: /system.slice/system-vncserver.slice/vncserver@:3.service
              └─ 8099 /usr/bin/Xvnc :3 -auth /root/.Xauthority -desktop n19dcat048-centos-domain:3 (root)...

Dec 01 09:11:20 n19dcat048-centos-domain systemd[1]: Starting Remote desktop service (VNC)...
Dec 01 09:11:20 n19dcat048-centos-domain systemd[1]: Started Remote desktop service (VNC).
```

Bước: 6 Truy cập phiên máy tính từ xa.

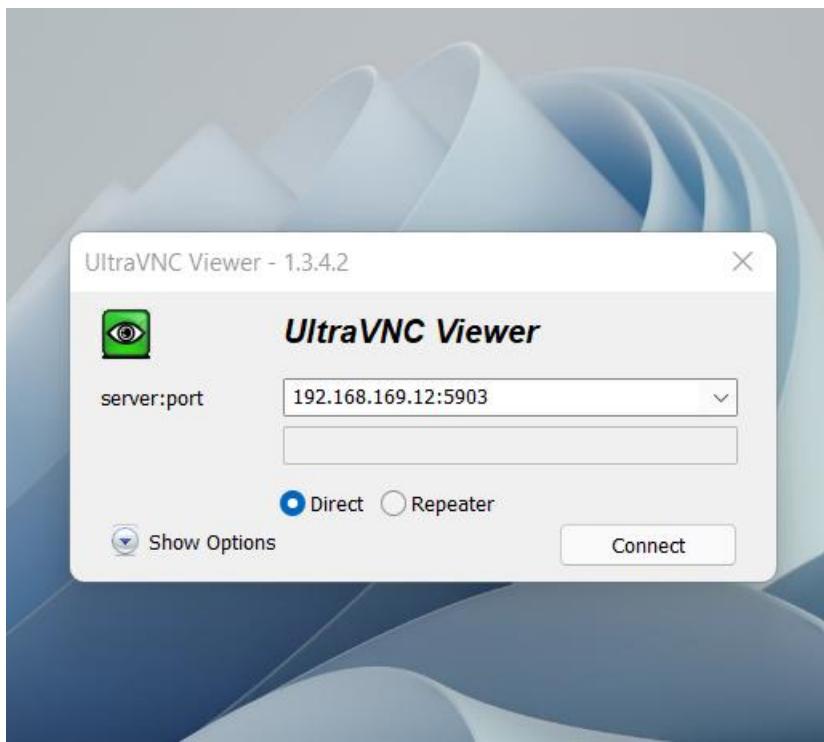
Từ Máy Centos:

```
[root@n19dcat048-centos-domain ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.169.12  netmask 255.255.255.0  broadcast 192.168.169.255
        inet6 fe80::373e:bc33:629e:f408  prefixlen 64  scopeid 0x20<link>
          ether 00:0c:29:79:b9:5a  txqueuelen 1000  (Ethernet)
            RX packets 110738  bytes 155243938 (148.0 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 30739  bytes 1906283 (1.8 MiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

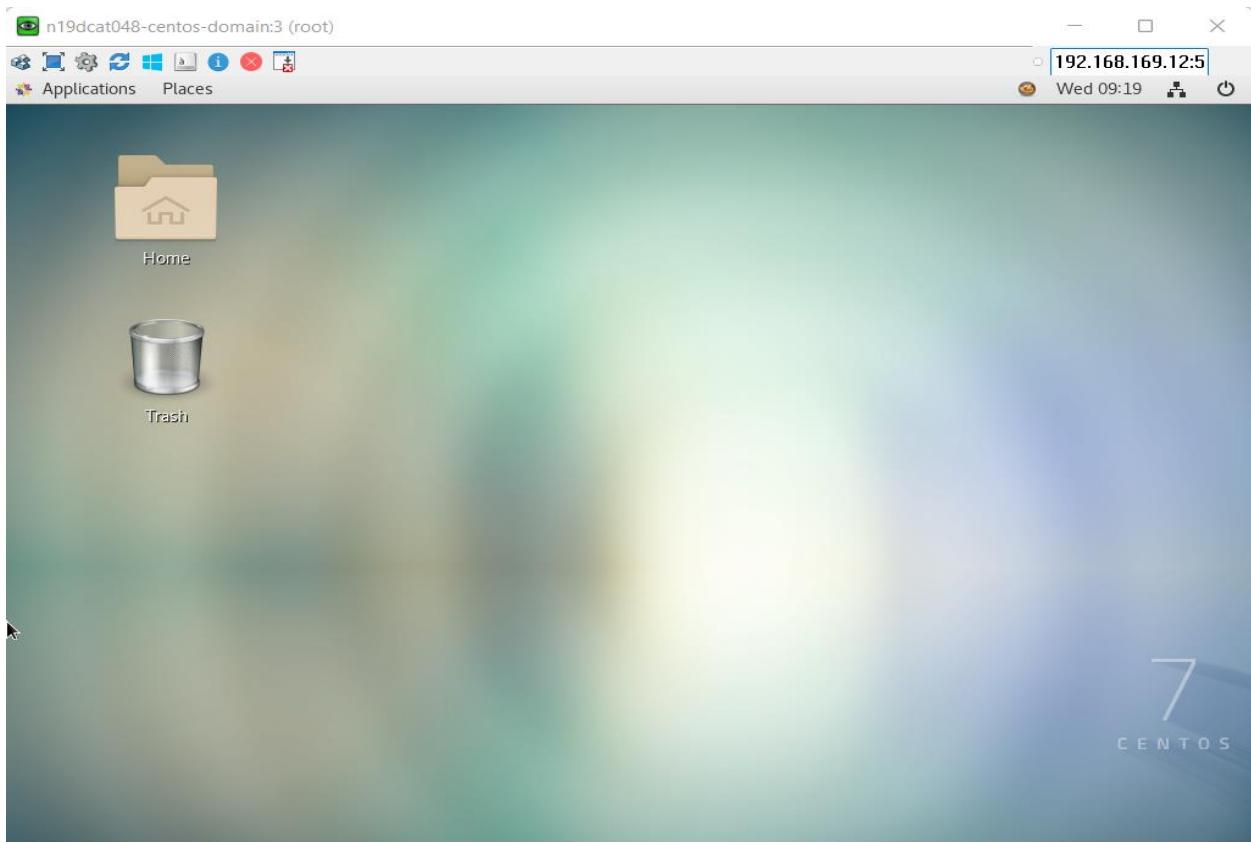
Nhập mật khẩu VNC mà chúng ta đã đặt ở bước trên, sau khi xác thực, phiên Remote Desktop sẽ bắt đầu.

Từ máy Windows bằng VNC Viewer

Nhập địa chỉ IP máy chủ VNC và số cổng, sau đó nhấn vào OK



Kết nối thành công.



2.5 Dịch vụ SSH

a. Giới thiệu

Secure Shell (SSH) là một giao thức mạng được sử dụng cho kết nối an toàn giữa máy khách và máy chủ. Mọi tương tác giữa máy chủ và máy khách đều được mã hóa. Hướng dẫn này giải thích cách bật SSH trên máy Ubuntu. Bật SSH sẽ cho phép bạn kết nối với hệ thống của mình từ xa và thực hiện các tác vụ quản trị. Bạn cũng sẽ có thể chuyển các tệp một cách an toàn qua scp và sftp.

b. Cài đặt SSH trên Ubuntu 20.04

Theo mặc định, khi Ubuntu được cài đặt lần đầu, nó không cho phép truy cập từ xa qua SSH. Việc cài đặt và kích hoạt SSH trên Ubuntu khá đơn giản. Thực hiện các bước sau với tư cách là người dùng root hoặc

người dùng có đặc quyền sudo để cài đặt và kích hoạt SSH trên hệ thống Ubuntu của bạn. Mở cửa sổ dòng lệnh với Ctrl+Alt+T và cài đặt gói openssh-server.

```
nguyencongluc@infosec:~$ sudo apt update
[sudo] password for nguyencongluc:
Hit:1 http://vn.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://vn.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [570 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1.387 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [281 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [277 kB]
Get:9 http://vn.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [14,6 kB]
```

- Khi được nhắc, hãy nhập mật khẩu của bạn và nhấn Enter để tiếp tục cài đặt

```
nguyencongluc@infosec:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:8.2p1-4ubuntu0.3).
openssh-server set to manually installed.
```

- Sau khi cài đặt xong, dịch vụ SSH sẽ tự động khởi động. Bạn có thể xác minh rằng SSH đang chạy bằng cách gõ lệnh sau.

```
nguyencongluc@infosec:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2021-12-01 09:29:29 +07; 3min 41s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 905 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 917 (sshd)
   Tasks: 1 (limit: 2260)
  Memory: 1.9M
   CGroup: /system.slice/ssh.service
           └─ 917 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Thg 12 01 09:29:29 infosec systemd[1]: Starting OpenBSD Secure Shell server...
Thg 12 01 09:29:29 infosec sshd[917]: Server listening on 0.0.0.0 port 22
```

- Đầu ra sẽ cho bạn biết rằng dịch vụ đang chạy và đã được kích hoạt để tự động khởi động khi hệ thống bắt đầu khởi động.

- Nhấn q để quay lại dấu nhắc dòng lệnh. Ubuntu đi kèm với một công cụ cấu hình tường lửa được gọi là UFW. Nếu tường lửa được bật trên hệ thống của bạn, hãy đảm bảo rằng bạn đã mở cổng SSH.

```
nguyencongluc@infosec:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
nguyencongluc@infosec:~$
```

- Bây giờ bạn có thể kết nối với hệ thống Ubuntu của mình thông qua SSH từ bất kỳ máy từ xa nào. Hệ thống Linux và macOS có các máy khách SSH được cài đặt theo mặc định. Để kết nối từ máy Windows, hãy sử dụng ứng dụng khách SSH như PuTTY.

c. Kết nối với máy chủ SSH

```
nguyencongluc@infosec:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:93:90:46 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
        inet 192.168.169.11/24 brd 192.168.169.255 scope global dynamic noprefixroute
            valid_lft 1771sec preferred_lft 1771sec
        inet6 fe80::bed3:f213:a7e4:5850/64 scope link noprefixroute
```

Mình đã setup xong, và đây là thông báo mặc định khi bạn kết nối với Ubuntu

```
C:\> Select nguyencongluc@infosec: ~
Microsoft Windows [Version 10.0.22000.318]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Nguyen Cong Luc>ssh nguyencongluc@192.168.169.11
The authenticity of host '192.168.169.11 (192.168.169.11)' can't be established.
ECDSA key fingerprint is SHA256:0ysRU6oXVrQ1jZ0tDdl3Llx0WyV+DCDCKGARMbq5B74.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Y
Please type 'yes', 'no' or the fingerprint: Yes
Warning: Permanently added '192.168.169.11' (ECDSA) to the list of known hosts.
nguyencongluc@192.168.169.11's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-41-generic x86_64)

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

0 updates can be applied immediately.

Your Hardware Enablement Stack (HWE) is supported until April 2025.

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.

nguyencongluc@infosec:~$
```

d. Tắt/Mở SSH trên Ubuntu

Để tắt máy chủ SSH trên hệ thống Ubuntu của bạn, chỉ cần dừng lại dịch vụ SSH bằng cách chạy lệnh sau. Sudo systemctl disable --now ssh Sau đó để kích hoạt lại nó, hãy nhập: sudo systemctl enable --now ssh

```
nguyencongluc@infosec:~$ sudo systemctl disable --now ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sys-
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable ssh
Removed /etc/systemd/system/multi-user.target.wants/ssh.service.
Removed /etc/systemd/system/sshd.service.
```

```
nguyencongluc@infosec:~$ sudo systemctl enable --now ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sys-
temd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.servi-
ce.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/sy-
stemd/system/ssh.service.
```

2.6. Dịch vụ DNS và DHCP

a. Dịch vụ DNS:

Tham khảo: <https://adminvietnam.org/cau-hinh-dns-tren-centos-7/2218/>

b. Dịch vụ DHCP:

Tham khảo: <https://cuongquach.com/cai-dat-va-cau-hinh-dhcp-server-tren-centos-7.html>

2.7. Dịch vụ thư điện tử

2.8. Quản lý User và Group

a. Quản lý User

Để quản lý User. Ví dụ ta có 1 group lucsky

```
root@infosec:~# groupadd lucsky
root@infosec:~#
```

Thêm user vào group

useradd: tạo user

-c: comment (chú thích)

-d: home directory (thư mục cá nhân)

-G: đưa user vào group

-M: không tạo thư mục cá nhân

-n: không tạo primary group, user tạo ra sẽ được đưa vào group users

-s: chỉ định shell

Tạo user

```
nguyencongluc@infosec:~$ sudo -i  
root@infosec:~# useradd user1
```

Đưa user1 vừa tạo vào group lucsky

```
root@infosec:~# usermod -G lucsky user1  
root@infosec:~#
```

Xóa user

```
root@infosec:~# userdel user1  
root@infosec:~#
```

Kiểm tra user1 sau khi xóa:

```
root@infosec:~# id user1  
id: 'user1': no such user  
root@infosec:~#
```

b. Quản lý Group

Tạo group: attt

Thêm user vào Group

Để thực hiện việc thêm user vào group ta tạo user tên: n19dcat048

Sau đó ta tiến hành lệnh thêm user vào group

```
root@infosec:~# groupadd attt  
root@infosec:~# useradd n19dcat048  
root@infosec:~# usermod -a -G attt n19dcat048  
root@infosec:~#
```

Kiểm tra id user vừa thêm

```
root@infosec:~# id n19dcat048  
uid=1001(n19dcat048) gid=1001(n19dcat048) groups=1001(n19dcat048),1004(attt)  
root@infosec:~#
```

Xóa Group

```
root@infosec:~# groupdel attt  
root@infosec:~#  
root@infosec:~# groups attt  
groups: 'attt': no such user  
root@infosec:~#
```

c. File lưu trữ dữ liệu về User và Group

File /etc/shadow

Gắn với file /etc/passwd là file /etc/shadow. Nó là phương thức khác của Linux để lưu thông tin mật khẩu đăng nhập người dùng trên hệ thống. Thông tin được lưu tại đây sẽ an toàn hơn so với cách lưu

trong tập tin /etc/passwd do tập tin này chỉ có tài khoản root hoặc có quyền sudo mới có thể truy cập.
Để xem dòng đầu tiên của file: /etc/shadow

```
root@infosec:~# cat /etc/shadow | head -1
root:!$1$18899$0:99999:7:::
root@infosec:~#
```

Đối với file /etc/shadow gồm có 8 trường:

Trường 1: Chính là username root

Trường thứ 2: Chính là password đã được mã hóa. Đây là một thuật toán
băm.

Trường thứ 3: Là khoảng thời gian (tính bằng ngày) tính từ 1/1/1970 cho tới
lần đổi mật khẩu gần nhất.

Trường thứ 4: Thời gian tối đa còn cho phép người dùng đổi mật khẩu, nếu
là 0 tức là người dùng có thể đổi mật khẩu bất cứ khi nào, nếu là số khác 0,
ví dụ 5, tức là người dùng còn 5 ngày nữa có thể đổi mật khẩu.

Trường thứ 5: Thời gian hiệu lực tối đa của mật khẩu, nếu là 99999 có nghĩa
là vô hạn.

Trường thứ 6: Khoảng thời gian trước khi mật khẩu hết hạn, hệ thống sẽ cảnh
báo cho người dùng, ở đây là 7, tức là trước khi hết hạn 7 ngày, hệ thống sẽ
cảnh báo.

Trường thứ 7: Khoảng thời gian tài khoản hết hạn đăng nhập.

Trường thứ 8: Thời gian mà tài khoản đã hết hạn đăng nhập tính từ ngày
1/1/1970 (đơn vị tính là ngày).

File /etc/passwd

File passwd nằm ở thư mục /etc chứa danh sách tài khoản trên hệ thống, cung cấp thông tin về mỗi tài
khoản như: User ID, Group ID, Home Directory, Shell...

Định dạng của file /etc/passwd mỗi dòng trong file là thông tin 1 user. Có tất cả 7 trường trên mỗi dòng,
các trường được phân tách bởi dấu 2 chấm (:).

Dưới đây là 1 ví dụ về thông tin của một user.

Xem dòng đầu tiên của file: /etc/passwd

```
root@infosec:~# cat /etc/passwd | head -1
root:x:0:0:root:/root:/bin/bash
root@infosec:~#
```

Ý nghĩa của 7 trường như sau:

Trường 1 Username: Tên người dùng, được sử dụng khi user đăng nhập, không nên chứa các ký tự in hoa trong username. Nó có độ dài từ 1 đến 32 ký tự.

Trường 2 Password: Nếu sử dụng shadow password thì nên sử dụng dấu x hoặc ký tự *

Trường 3 User ID (UID): Đây là 1 chuỗi số duy nhất được gán cho user, hệ thống sử dụng UID hơn là username để nhận dạng user.

Trường 4 Group ID (GID): Là 1 chuỗi số duy nhất được gán cho Group đầu tiên mà user này tham gia.

Trường 5 User ID Info: Dùng mô tả người dùng ví dụ như: địa chỉ, sdt,...

Trường 6 Home directory: Đường dẫn tuyệt đối đến thư mục mà người dùng sẽ ở khi họ đăng nhập. Nếu thư mục này không tồn tại thì thư mục người dùng sẽ trở thành /

Trường 7 Shell: Đường dẫn tuyệt đối của lệnh hoặc shell (/ bin / bash).

File /etc/shadow

File /etc/group chứa các thuộc tính nhóm cơ bản. Đây là file ASCII chứa các bản ghi các nhóm trên hệ thống. Mỗi bản ghi xuất hiện trên một dòng duy nhất:

Để xem dòng đầu tiên của file /etc/group

```
root@infosec:~# cat /etc/group | head -1
root:x:0:
root@infosec:~#
```

File /etc/group có 4 trường:

Trường 1 groupname: Chứa tên được gán cho nhóm.

Trường 2 group-password: x trong trường này cho biết mật khẩu shadow được sử dụng.

Trường 3 GID: Chứa số GID của nhóm.

Trường 4 group-password: Danh sách người dùng là thành viên của nhóm.

Chú ý: Mỗi nhóm có thể có nhiều người dùng. Người dùng cũng có thể thuộc một hay nhiều nhóm.

File /etc/skel

File /etc/skel được sử dụng để bắt đầu thư mục chính khi người dùng được tạo lần đầu tiên. Cách bố trí mẫu của các file người dùng của skel được thể hiện dưới đây:

```
root@infosec:~# ls -lart /etc/skel
total 28
-rw-r--r--  1 root root   807 Thg 2  25  2020 .profile
-rw-r--r--  1 root root  3771 Thg 2  25  2020 .bashrc
-rw-r--r--  1 root root   220 Thg 2  25  2020 .bash_logout
drwxr-xr-x  2 root root  4096 Thg 8  19 17:30 .
drwxr-xr-x 135 root root 12288 Thg 12  1 09:57 ..
root@infosec:~#
```

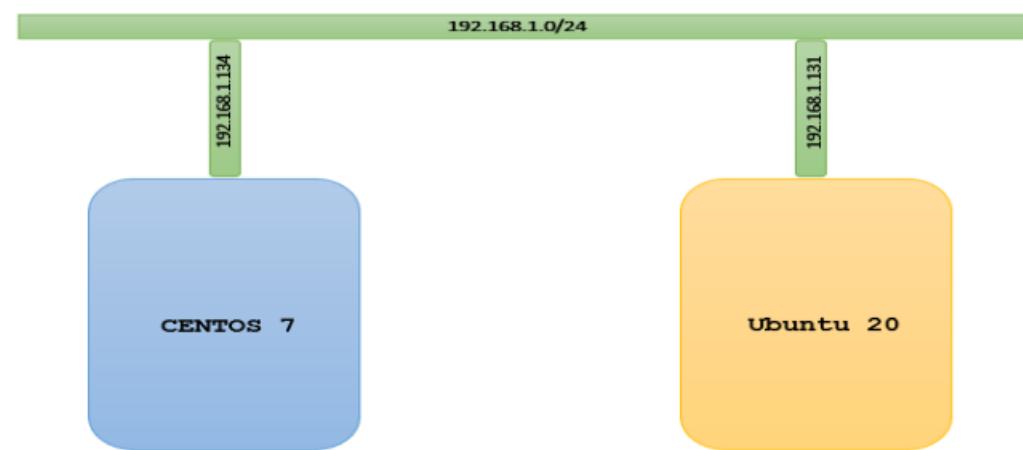
Quyền mặc định của thư mục /etc/skel là drwxr-xr-x. Không nên thay đổi quyền của skel hoặc nội dung của nó. Thay đổi quyền có thể có thể phá vỡ một số chương trình, bởi vì trong thư mục skel có một số cấu hình cần sự cho phép đọc và cấp cho nó quyền thực thi sẽ làm một số chương trình hoạt động.

2.9. Dịch vụ web

* Sử dụng tool Nagios để giám sát 1 trang web, nếu bị mất liên lạc thì gửi mail để thông báo

a. Chuẩn bị

Chuẩn bị môi trường cài đặt



b. Cài đặt Nagios trên CentOS 7

Cài đặt các gói chuẩn bị cần thiết Để có thể cài đặt và sử dụng được Nagios Core, chúng ta phải cài đặt một số thư viện và các gói thư viện dịch vụ đi kèm.

Bước 1: Cài đặt các gói thư viện

```
[root@n19dcat048-centos-domain ~]# yum install gcc glibc glibc-common gd gd-devel make net-snmp openssl-devel xinetd unzip httpd php php-fpm curl wget -y
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.math.princeton.edu
 * extras: or-mirror.iwebfusion.net
 * updates: mirror.phx1.us.spryservers.net
Package 1:make-3.82-24.el7.x86_64 already installed and latest version
No package xinetd available.
No package php-fpm available.
Package wget-1.14-18.el7_6.1.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
--> Package curl.x86_64 0:7.29.0-59.el7 will be updated
--> Package curl.x86_64 0:7.29.0-59.el7_9.1 will be an update
--> Processing Dependency: libcurl = 7.29.0-59.el7_9.1 for package: curl-7.29.0-59.el7_9.1.x86_64
--> Package gcc.x86_64 0:4.8.5-44.el7 will be installed
--> Processing Dependency: cpp = 4.8.5-44.el7 for package: gcc-4.8.5-44.el7.x86_64
--> Processing Dependency: glibc-devel >= 2.2.90-12 for package: gcc-4.8.5-44.el7.x86_64
--> Package gd.x86_64 0:2.0.35-26.el7 will be updated
```

Bước 2: Mở port 80 cho HTTPD trên Firewalld

Nếu server của bạn có sử dụng Firewalld, hãy mở port cho httpd bằng lệnh:

```
[root@n19dcat048-centos-domain ~]# firewall-cmd --permanent --add-port=80/tcp
success
[root@n19dcat048-centos-domain ~]# firewall-cmd --reload
success
[root@n19dcat048-centos-domain ~]# █
```

Bước 3: Tắt SELinux

Tắt tức thời bằng lệnh:

```
[root@n19dcat048-centos-domain ~]# setenforce 0
[root@n19dcat048-centos-domain ~]# █
```

Chỉnh sửa file cấu hình của SELinux:

```
[root@n19dcat048-centos-domain ~]# vi /etc/sysconfig/selinux
```

Sửa dòng SELINUX=enforcing thành SELINUX=disable.

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Tạo user cho Nagios

Tạo user nagios trên máy chủ cài đặt Nagios Server

```
[root@n19dcat048-centos-domain ~]# useradd -m -s /bin/bash nagios
[root@n19dcat048-centos-domain ~]# █
```

Tạo group nagcmd cho phép sử dụng thư mục Web UI, thêm nagios và apache:

```
[root@n19dcat048-centos-domain ~]# groupadd nagcmd
[root@n19dcat048-centos-domain ~]# usermod -a -G nagcmd nagios
[root@n19dcat048-centos-domain ~]# usermod -a -G nagcmd apache
[root@n19dcat048-centos-domain ~]#
```

Cài đặt Nagios Core và Plugin

Tải gói Plugin và giải nén

Chúng ta tải Nagios Core về server. Tại thời điểm viết bài, phiên bản mới nhất là Nagios Core 4.3.1.

```
[root@n19dcat048-centos-domain nagios-4.3.1]# cd /opt
[root@n19dcat048-centos-domain opt]# █
```

```
[root@n19dcat048-centos-domain opt]# wget https://nagios-plugins.org/download/nagios-plugins-2.2.0.tar.gz --no-check-certificate
--2021-12-01 10:48:32-- https://nagios-plugins.org/download/nagios-plugins-2.2.0.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:443... connected.
WARNING: cannot verify nagios-plugins.org's certificate, issued by '/C=US/O=Let's Encrypt/CN=R3':
Issued certificate has expired.
HTTP request sent, awaiting response... 200 OK
Length: 2725282 (2.6M) [application/x-gzip]
Saving to: 'nagios-plugins-2.2.0.tar.gz'

100%[=====] 2,725,282 1.38MB/s in 1.9s
2021-12-01 10:48:35 (1.38 MB/s) - 'nagios-plugins-2.2.0.tar.gz' saved [2725282/2725282]

[root@n19dcat048-centos-domain opt]# █
```

```
[root@n19dcat048-centos-domain opt]# wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.3.1.tar.gz
--2021-12-01 11:06:29-- http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.3.1.tar.gz
Resolving prdownloads.sourceforge.net (prdownloads.sourceforge.net)... 204.68.111.105
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|204.68.111.105|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.3.1/nagios-4.3.1.tar.gz [following]
--2021-12-01 11:06:29-- http://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.3.1/nagios-4.3.1.tar.gz
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 204.68.111.105
Reusing existing connection to prdownloads.sourceforge.net:80.
HTTP request sent, awaiting response... 302 Found
Location: http://iweb.dl.sourceforge.net/project/nagios/nagios-4.x/nagios-4.3.1/nagios-4.3.1.tar.gz [following]
--2021-12-01 11:06:30-- http://iweb.dl.sourceforge.net/project/nagios/nagios-4.x/nagios-4.3.1/nagios-4.3.1.tar.gz
Resolving iweb.dl.sourceforge.net (iweb.dl.sourceforge.net)... 192.175.120.182, 2607:f748:10:12::5f:2
Connecting to iweb.dl.sourceforge.net (iweb.dl.sourceforge.net)|192.175.120.182|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11095797 (11M) [application/x-gzip]
Saving to: 'nagios-4.3.1.tar.gz.1'

100%[=====] 11,095,797 2.08MB/s in 7.0s
2021-12-01 11:06:37 (1.52 MB/s) - 'nagios-4.3.1.tar.gz.1' saved [11095797/11095797]

[root@n19dcat048-centos-domain opt]# █
```

Bước 1: Giải nén source Nagios

```
[root@n19dcat048-centos-domain opt]# tar xf nagios-4.3.1.tar.gz
```

Bước 2: Biên dịch Nagios

- Thứ tự thực hiện các lệnh:

```
cd nagios-4.3.1  
./configure --with-command-group=nagcmd  
make all  
make install  
make install-commandmode  
make install-init  
make install-config  
make install-webconf
```

```
[root@n19dcat048-centos-domain opt]# cd nagios-4.3.1  
[root@n19dcat048-centos-domain nagios-4.3.1]# ./configure --with-command-group=nagcmd  
checking for a BSD-compatible install... /bin/install -c  
checking build system type... x86_64-pc-linux-gnu  
checking host system type... x86_64-pc-linux-gnu  
checking for gcc... gcc  
checking whether the C compiler works... yes  
checking for C compiler default output file name... a.out  
checking for suffix of executables...  
checking whether we are cross compiling... no  
checking for suffix of object files... o  
checking whether we are using the GNU C compiler... yes  
checking whether gcc accepts -g... yes  
checking for gcc option to accept ISO C89... none needed  
checking whether make sets $(MAKE)... yes
```

```
[root@n19dcat048-centos-domain nagios-4.3.1]# make all  
cd ./base && make  
make[1]: Entering directory `/opt/nagios-4.3.1/base'  
make -C ../lib  
make[2]: Entering directory `/opt/nagios-4.3.1/lib'  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c squeue.c -o squeue.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c kvvec.c -o kvvec.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c iocache.c -o iocache.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c iobroker.c -o iobroker.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c bitmap.c -o bitmap.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c dkhash.c -o dkhash.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c runcmd.c -o runcmd.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c nsutils.c -o nsutils.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c fanout.c -o fanout.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c pqueue.c -o pqueue.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c worker.c -o worker.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c skiplist.c -o skiplist.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c nsock.c -o nsock.o  
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c nspath.c -o nspath.o
```

```
[root@n19dcat048-centos-domain nagios-4.3.1]# make install
cd ./base && make install
make[1]: Entering directory `/opt/nagios-4.3.1/base'
make install-basic
make[2]: Entering directory `/opt/nagios-4.3.1/base'
/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/bin/install -c -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/bin/install -c -m 774 -o nagios -g nagios nagiostats /usr/local/nagios/bin
make[2]: Leaving directory `/opt/nagios-4.3.1/base'
make strip-post-install
make[2]: Entering directory `/opt/nagios-4.3.1/base'
/bin/strip /usr/local/nagios/bin/nagios
/bin/strip /usr/local/nagios/bin/nagiostats
make[2]: Leaving directory `/opt/nagios-4.3.1/base'
make[1]: Leaving directory `/opt/nagios-4.3.1/base'
cd ./cgi && make install
make[1]: Entering directory `/opt/nagios-4.3.1/cgi'
make install-basic
make[2]: Entering directory `/opt/nagios-4.3.1/cgi'
/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/sbin
for file in *.cgi; do \
    /bin/install -c -m 775 -o nagios -g nagios $file /usr/local/nagios/sbin; \
done
```

Bước 3: Cho phép nagios khởi động cùng với hệ thống:

```
[root@n19dcat048-centos-domain nagios-4.3.1]# make install-commandmode
/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

[root@n19dcat048-centos-domain nagios-4.3.1]# █
```

```
[root@n19dcat048-centos-domain nagios-4.3.1]# make install-init
/bin/install -c -m 755 -d -o root -g root /etc/rc.d/init.d
/bin/install -c -m 755 -o root -g root daemon-init /etc/rc.d/init.d/nagios

*** Init script installed ***

[root@n19dcat048-centos-domain nagios-4.3.1]# █

[root@n19dcat048-centos-domain nagios-4.3.1]# make install-config
/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg /usr/local/nagios/etc/cgi.cfg
/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagi
```

```
[root@n19dcat048-centos-domain nagios-4.3.1]# make install-webconf
/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf
if [ 0 -eq 1 ]; then \
    ln -s /etc/httpd/conf.d/nagios.conf /etc/apache2/sites-enabled/nagios.conf; \
fi

*** Nagios/Apache conf file installed ***

[root@n19dcat048-centos-domain nagios-4.3.1]#
```

Bước 4: Cài đặt password cho nagiosadmin, khi đăng nhập Web:

```
[root@n19dcat048-centos-domain nagios-4.3.1]# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
[root@n19dcat048-centos-domain nagios-4.3.1]#
```

Bước 5: Tải gói Plugin và giải nén

```
[root@n19dcat048-centos-domain opt]# wget https://nagios-plugins.org/download/nagios-plugins-2.2.0.tar.gz --no-check-certificate
--2021-12-01 11:29:10-- https://nagios-plugins.org/download/nagios-plugins-2.2.0.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:443... connected.
WARNING: cannot verify nagios-plugins.org's certificate, issued by '/C=US/O=Let's Encrypt/CN=R3':
Issued certificate has expired.
HTTP request sent, awaiting response... 200 OK
Length: 2725282 (2.6M) [application/x-gzip]
Saving to: 'nagios-plugins-2.2.0.tar.gz.2'

100%[=====] 2,725,282      531KB/s   in 7.1s

2021-12-01 11:29:19 (374 KB/s) - 'nagios-plugins-2.2.0.tar.gz.2' saved [2725282/2725282]

[root@n19dcat048-centos-domain opt]# tar xzf nagios-plugins-2.2.0.tar.gz
[root@n19dcat048-centos-domain opt]#
```

Bước 6: Biên dịch các Plugin từ source code

```
cd nagios-plugins-2.2.0
./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl
make
make install
```

```
[root@n19dcat048-centos-domain nagios-plugins-2.2.0]# ./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl
checking for a BSD-compatible install... /bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether to disable maintainer-specific portions of Makefiles... yes
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /bin/grep
```

```
[root@n19dcat048-centos-domain nagios-plugins-2.2.0]# make
make all-recursive
make[1]: Entering directory `/opt/nagios-plugins-2.2.0'
Making all in gl
make[2]: Entering directory `/opt/nagios-plugins-2.2.0/gl'
rm -f alloca.h-t alloca.h && \
{ echo '/* DO NOT EDIT! GENERATED AUTOMATICALLY! */'; \
cat ./alloca.in.h; \
} > alloca.h-t && \
mv -f alloca.h-t alloca.h
rm -f c++defs.h-t c++defs.h && \
sed -n -e '/_GL_CXXDEFS/, $p' \
< ../build-aux/snippet/c++defs.h \
> c++defs.h-t && \
mv c++defs.h-t c++defs.h
rm -f warn-on-use.h-t warn-on-use.h && \
sed -n -e '/^.\ ifndef/, $p' \
< ../build-aux/snippet/warn-on-use.h \
> warn-on-use.h-t && \
mv warn-on-use.h-t warn-on-use.h
rm -f arg-nonnull.h-t arg-nonnull.h && \
sed -n -e '/_GL_ARG_NONNULL/, $p' \
< ../build-aux/snippet/arg-nonnull.h \
> arg-nonnull.h-t && \

```

Khởi động Nagios Server

Khởi động lại Apache và chạy nagios, cho phép khởi động cùng hệ thống:

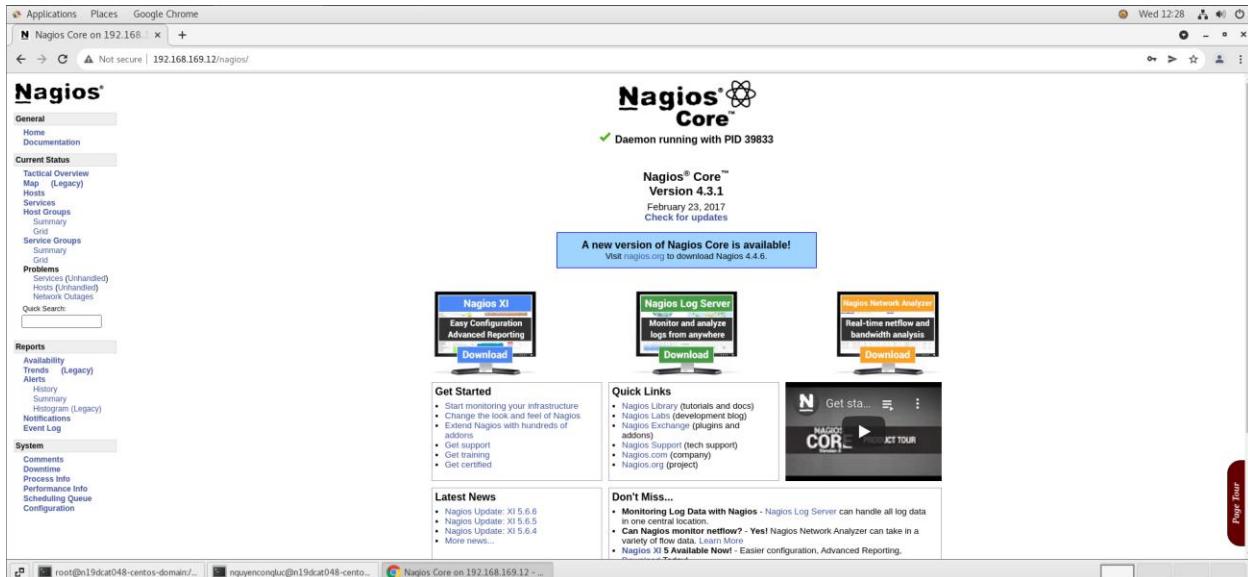
```
make[2]: Leaving directory `/opt/nagios-plugins-2.2.0'
make[1]: Leaving directory `/opt/nagios-plugins-2.2.0'
[root@n19dcat048-centos-domain nagios-plugins-2.2.0]# clear

[root@n19dcat048-centos-domain nagios-plugins-2.2.0]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@n19dcat048-centos-domain nagios-plugins-2.2.0]# systemctl restart httpd
[root@n19dcat048-centos-domain nagios-plugins-2.2.0]# service nagios restart
Restarting nagios (via systemctl): [ OK ]
[root@n19dcat048-centos-domain nagios-plugins-2.2.0]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
     Active: active (running) since Wed 2021-12-01 12:06:21 +07; 53s ago
       Docs: man:httpd(8)
              man:apachectl(8)
    Main PID: 39774 (httpd)
      Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
      Tasks: 6
     CGroup: /system.slice/httpd.service
             ├─39774 /usr/sbin/httpd -DFOREGROUND
             ├─39779 /usr/sbin/httpd -DFOREGROUND
             ├─39780 /usr/sbin/httpd -DFOREGROUND
             ├─39781 /usr/sbin/httpd -DFOREGROUND
             ├─39782 /usr/sbin/httpd -DFOREGROUND
             └─39783 /usr/sbin/httpd -DFOREGROUND

Dec 01 12:06:16 n19dcat048-centos-domain systemd[1]: Starting The Apache HTTP Server...
Dec 01 12:06:20 n19dcat048-centos-domain httpd[39774]: AH00558: httpd: Could not reliably determine...ge
Dec 01 12:06:21 n19dcat048-centos-domain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@n19dcat048-centos-domain nagios-plugins-2.2.0]# 
```

Để kiểm tra, hãy truy cập vào giao diện Web và đăng nhập bằng tài khoản nagiosadmin và Password vừa tạo ở địa chỉ:

<http://192.168.169.12/nagios/>



c. Giám sát thông qua NRPE

c.1 Cài đặt NRPE trên Nagios Server

NRPE - (Nagios Remote Plugin Executor) là một công cụ đi kèm để theo dõi tài nguyên hệ thống, nó còn được biết như một Agent để theo dõi các host từ xa (Remote hosts).

Mục đích của việc cài đặt này là để biên dịch ra plugin check_nrpe.

Bước 1: Tải và Giải nén source gói NRPE

```
cd /opt
curl -L -O http://downloads.sourceforge.net/project/nagios/nrpe-2.x/nrpe-2.15/nrpe-2.15.tar.gz

tar xf nrpe-*.tar.gz
```

```
[root@n19dcat048-centos-domain ~]# cd /opt
[root@n19dcat048-centos-domain opt]# curl -L -O http://downloads.sourceforge.net/project/nagios/nrpe-2.x/nrpe-2.15/nrpe-2.15.tar.gz
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total   Spent   Left Speed
100  351  100  351    0      0  727    0 --:--:-- --:--:-- --:--:--  728
100 409k  100 409k    0      0 130k    0 0:00:03 0:00:03 --:--:-- 150k
[root@n19dcat048-centos-domain opt]# tar xf nrpe-*.tar.gz
[root@n19dcat048-centos-domain opt]#
```

Bước 2: Biên dịch NRPE từ source

```
[root@n19dcat048-centos-domain nrpe-2.15]# ./configure --enable-command-args --with-nagios-user=nagios \
> --with-nagios-group=nagios --with-ssl=/usr/bin/openssl \
> --with-ssl-lib=/usr/lib/x86_64-linux-gnu
checking for a BSD-compatible install... /bin/install -c
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ANSI C... none needed
checking whether make sets $(MAKE)... yes
checking how to run the C preprocessor... gcc -E
checking for egrep... grep -E
checking for ANSI C header files... yes
checking whether time.h and sys/time.h may both be included... yes
checking for sys/wait.h that is POSIX.1 compatible... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.h... yes
checking ctype.h usability... yes
checking ctype.h presence... yes
```

```
+.....+.....+.....+....+
+.....+.....+.....+....+
.....+.....+.....+....+
...+...++*++*++*++*++*
checking for Kerberos include files... could not find include files
checking for perl... /bin/perl
configure: creating ./config.status
config.status: creating Makefile
config.status: creating subst
config.status: creating src/Makefile
config.status: creating package/solaris/Makefile
config.status: creating init-script
config.status: creating init-script.debian
config.status: creating init-script.suse
config.status: creating nrpe.spec
config.status: creating sample-config/nrpe.cfg
config.status: creating sample-config/nrpe.xinetd
config.status: creating include/config.h
config.status: include/config.h is unchanged
```

```
*** Configuration summary for nrpe 2.15 09-06-2013 ***:
```

General Options:

```
-----
```

```
NRPE port: 5666
NRPE user: nagios
NRPE group: nagios
Nagios user: nagios
Nagios group: nagios
```

Review the options above for accuracy. If they look okay,
type 'make all' to compile the NRPE daemon and client.

```
[root@n19dcat048-centos-domain nrpe-2.15]# █
```

```
[root@n19dcat048-centos-domain nrpe-2.15]# make all
cd ./src/; make ; cd ..
make[1]: Entering directory `/opt/nrpe-2.15/src'
gcc -g -O2 -I/usr/include/openssl -I/usr/include -DHAVE_CONFIG_H -I ../include -I ../../include -o nrpe .
nrpe.c ./utils.c ./acl.c -L/usr/lib64 -lssl -lcrypto -lnsl
gcc -g -O2 -I/usr/include/openssl -I/usr/include -DHAVE_CONFIG_H -I ../include -I ../../include -o check_
nrpe ./check_nrpe.c ./utils.c -L/usr/lib64 -lssl -lcrypto -lnsl
make[1]: Leaving directory `/opt/nrpe-2.15/src'
```

```
*** Compile finished ***
```

If the NRPE daemon and client compiled without any errors, you
can continue with the installation or upgrade process.

Read the PDF documentation (NRPE.pdf) for information on the next
steps you should take to complete the installation or upgrade.

```
[root@n19dcat048-centos-domain nrpe-2.15]# make install
cd ./src/ && make install
make[1]: Entering directory `/opt/nrpe-2.15/src'
make install-plugin
make[2]: Entering directory `/opt/nrpe-2.15/src'
/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/libexec
/bin/install -c -m 775 -o nagios -g nagios check_nrpe /usr/local/nagios/libexec
make[2]: Leaving directory `/opt/nrpe-2.15/src'
make install-daemon
make[2]: Entering directory `/opt/nrpe-2.15/src'
/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/bin/install -c -m 775 -o nagios -g nagios nrpe /usr/local/nagios/bin
make[2]: Leaving directory `/opt/nrpe-2.15/src'
make[1]: Leaving directory `/opt/nrpe-2.15/src'
[root@n19dcat048-centos-domain nrpe-2.15]#
```

Bước 3: Thêm câu lệnh check_nrpe

Mở file vi /usr/local/nagios/etc/objects/commands.cfg:

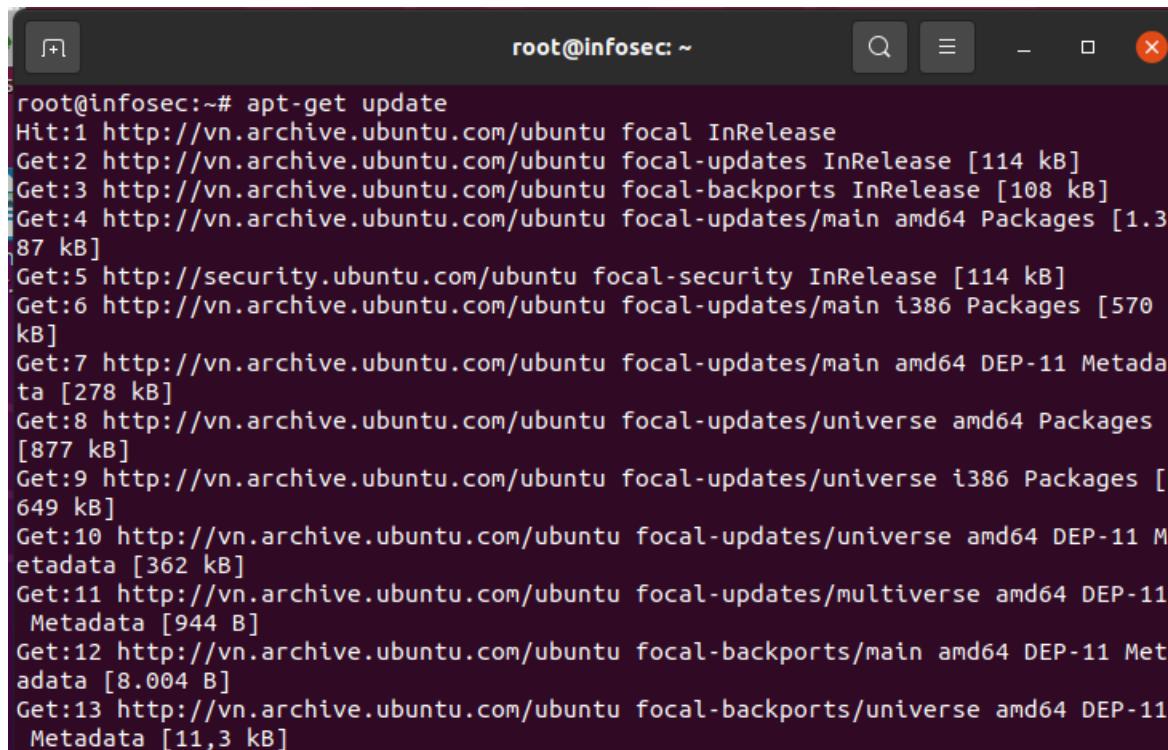
```
[root@n19dcat048-centos-domain nrpe-2.15]# vi /usr/local/nagios/etc/objects/commands.cfg
```

- Thêm câu lệnh sau vào cuối file:

c.2 Cài đặt NRPE trên host cần giám sát

Trên host Linux cần giám sát, chúng ta cần thực hiện các bước sau:

Bước 1: Cập nhật repo cho host



```
root@infosec:~# apt-get update
Hit:1 http://vn.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://vn.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1.387 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [570 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [278 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [877 kB]
Get:9 http://vn.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages [649 kB]
Get:10 http://vn.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [362 kB]
Get:11 http://vn.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [944 B]
Get:12 http://vn.archive.ubuntu.com/ubuntu focal-backports/main amd64 DEP-11 Metadata [8.004 B]
Get:13 http://vn.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [11,3 kB]
```

Bước 2: Cài đặt NRPE và các Plugin trên host cần giám sát

```
root@infosec:~# apt-get install nagios-plugins nagios-nrpe-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libdbi1 libnet-snmp-perl libpq5 libradcli4 libtirpc-common libtirpc3
  monitoring-plugins-basic monitoring-plugins-common
  monitoring-plugins-standard python3-crypto python3-gpg python3-samba
  python3-tdb rpcbind samba-common samba-common-bin samba-dsdb-modules
  smbclient snmp
Suggested packages:
  libcrypt-des-perl libdigest-hmac-perl libio-socket-inet6-perl icinga
  | icinga2 nagios-plugins-contrib fping postfix | sendmail-bin
  | exim4-daemon-heavy | exim4-daemon-light qstat xinetd | inetd
  heimdal-clients python3-markdown python3-dnspython cifs-utils
The following NEW packages will be installed:
  libdbi1 libnet-snmp-perl libpq5 libradcli4 libtirpc-common libtirpc3
  monitoring-plugins monitoring-plugins-basic monitoring-plugins-common
  monitoring-plugins-standard nagios-nrpe-server python3-crypto python3-gpg
```

Bước 3: Cấu hình NRPE trên host cần giám sát

Bước này có thể làm trên cả 2 distro CentOS và Ubuntu.

Sửa file cấu hình NRPE

```
root@infosec:~# vi /etc/nagios/nrpe.cfg
```

Tìm trường allowed_hosts và thêm địa chỉ IP Nagios server của bạn vào. Mỗi IP cách nhau bởi dấu phẩy (,):

```

define command{
    command_name      check_nt
    command_line      $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$ $ARG2$
}

#####
#
# SAMPLE PERFORMANCE DATA COMMANDS
#
# These are sample performance data commands that can be used to send performance
# data output to two text files (one for hosts, another for services). If you
# plan on simply writing performance data out to a file, consider using the
# host_perfdata_file and service_perfdata_file options in the main config file.
#
#####

# 'process-host-perfdata' command definition
define command{
    command_name      process-host-perfdata
    command_line      /usr/bin/printf "%b" "$LASTHOSTCHECK$\t$HOSTNAME$\t$HOSTSTATE$\t
.out
}

# 'process-service-perfdata' command definition
define command{
    command_name      process-service-perfdata
    command_line      /usr/bin/printf "%b" "$LASTSERVICECHECK$\t$HOSTNAME$\t$SERVICEDE
ICEPERFDATA$\n" >> /usr/local/nagios/var/service-perfdata.out
}

define command{
    command_name      check_nrpe
    command_line      $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}

```

Thoát và lưu lại file.

3.2 Cài đặt NRPE trên host cần giám sát

```
nguyencongluc@infosec:~$ sudo nano /etc/nagios/nrpe.cfg
```

Tìm trường allowed_hosts và thêm địa chỉ IP Nagios server của bạn vào. Mỗi IP cách nhau bởi dấu phẩy (,):

```
allowed_hosts=127.0.0.1, 192.168.3.19,::1
```

```

# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1, 192.168.169.12,::1

#
# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed. This option only works
# if the daemon was configured with the --enable-command-args configure script
# option.

```

Trong file đó tiếp tục khai báo câu lệnh cho NRPE.

Thêm câu lệnh để check các dịch vụ

Check 2 dịch vụ SSH và HTTP qua NRPE:

GNU nano 4.8	/etc/nagios/nrpe.cfg	Modified
<pre> # The following examples use hardcoded command arguments... # This is by far the most secure method of using NRPE command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10 command[check_load]=/usr/lib/nagios/plugins/check_load -r -w .15,.10,.05 -c .30> command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hd> command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200 command[check_http]=/usr/lib/nagios/plugins/check_http localhost command[check_ssh]=/usr/lib/nagios/plugins/check_ssh localhost # The following examples allow user-supplied arguments and can # only be used if the NRPE daemon was compiled with support for # command arguments *AND* the dont_blame_nrpe directive in this # config file is set to '1'. This poses a potential security risk, so # make sure you read the SECURITY file before doing this. ### MISC SYSTEM METRICS ### </pre>		

Để check các dịch vụ khác, chúng ta thêm câu lệnh tương tự với hướng dẫn bên trên. Lưu ý, cần chạy thử plugin trước để có hướng dẫn sử dụng.

```

root@infosec:~# service nagios-nrpe-server restart
root@infosec:~#

```

Sau khi cài đặt và cấu hình NRPE trên host mà chúng ta muốn giám sát, chúng ta cần phải thêm host đó vào cấu hình Nagios Server trước khi bắt đầu giám sát nó.

c.3 Thêm thông tin host trên Nagios Server

- Bước 1: Cấu hình Nagios Server

Chúng ta đặt tất cả các file cấu hình host giám sát vào một thư mục, sửa file cấu hình chính của nagios:

```
[root@n19dcat048-centos-domain ~]# nano /usr/local/nagios/etc/nagios.cfg
```

Tìm và bỏ "#" ở dòng:

```
...
cfg_dir=/usr/local/nagios/etc/servers
...
GNU nano 2.3.1      File: /usr/local/nagios/etc/nagios.cfg      Modified

#cfg_file=/usr/local/nagios/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg

# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

cfg_dir=/usr/local/nagios/etc/servers
cfg_dir=/usr/local/nagios/etc/printers
cfg_dir=/usr/local/nagios/etc/switches
cfg_dir=/usr/local/nagios/etc/routers

# OBJECT CACHE FILE

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^I Justify  ^W Where Is  ^V Next Page  ^U Uncut Text^T To Spell
```

Tạo thư mục để lưu trữ file cấu hình các host cần giám sát:

```
[root@n19dcat048-centos-domain ~]# mkdir /usr/local/nagios/etc/servers
[root@n19dcat048-centos-domain ~]#
```

- Bước 2: Tạo file cấu hình cho host giám sát trên Nagios Server

Trên Nagios Server, tạo file cấu hình cho mỗi host mà bạn muốn giám sát chúng ở folder /usr/local/nagios/etc/servers/. Trong trường hợp của tôi, tôi sẽ đặt tên cho nó là web01.cfg

Thêm nội dung sau vào file, phần host_name để định nghĩa ra một host mới, alias là phần mô tả ngắn về host; address là địa chỉ IP của host cần giám sát.

```
root@n19dcat048-centos-domain:~ - □ ×
File Edit View Search Terminal Help
GNU nano 2.3.1      File: /usr/local/nagios/etc/servers/web01.cfg      Modified
define host {
    use                  linux-server
    host_name           web01
    alias               My Apache server
    address             192.168.169.12
    max_check_attempts  5
    check_period        24x7
    notification_interval 30
    notification_period 24x7
}
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```

Với phần cấu hình trên, chúng ta chỉ có thể theo dõi được trạng thái UP/DOWN của host cần giám sát. Để giám sát thêm các dịch vụ, chúng ta tạo thêm các khối service trong phần cấu hình. check_command có thể được thêm và cài đặt các ngưỡng cảnh báo.

SSH:

```
define service {
    use          generic-service
    host_name    web01
    service_description SSHMonitor
    check_command check_nrpe!check_ssh
}
```

HTTP:

```
define service {
    use          generic-service
    host_name    web01
    service_description HTTPMonitor
```

```
check_command      check_nrpe!check_http
notifications_enabled  1
}
```

Chú thích:

- `use generic-service`: Sử dụng template có sẵn cho các dịch vụ
- `notifications_enabled 1`: Bật cảnh báo khi dịch vụ thay đổi trạng thái, 0 để tắt. Đây là file `web01.cfg` hoàn chỉnh, theo dõi 2 dịch vụ HTTP và SSH qua NRPE:

```

GNU nano 2.3.1      File: /usr/local/nagios/etc/servers/web01.cfg      Modified

define host {
    use                      linux-server
    host_name                web01
    alias                     My Apache server
    address                   192.168.169.12
    max_check_attempts        5
    check_period              24x7
    notification_interval     30
    notification_period       24x7
}
define service {
    use                      generic-service
    host_name                web01
    service_description       SSHMonitor
    check_command             check_nrpe!check_ssh
}
define service {
    use                      generic-service
    host_name                web01
}

```

```

GNU nano 2.3.1      File: /usr/local/nagios/etc/servers/web01.cfg      Modified

define service {
    use                      generic-service
    host_name                web01
    service_description       SSHMonitor
    check_command             check_nrpe!check_ssh
}
define service {
    use                      generic-service
    host_name                web01
    service_description       HTTPMonitor
    check_command             check_nrpe!check_http
}

```

Sau khi sửa xong, chúng ta lưu lại file và khởi động lại nagios server.

service nagios restart

```
[root@n19dcat048-centos-domain ~]# service nagios restart
Restarting nagios (via systemctl): [ OK ]
[root@n19dcat048-centos-domain ~]#
```

Kiểm tra trên Web UI của Nagios Server

Vào giao diện Web để kiểm tra lại:

<http://192.168.169.12/nagios>

Nagios Core on 192.168.1 x +

Not secure | 192.168.169.12/nagios/

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages
- Quick Search:

Reports

- Availability
- Trends (Legacy)
- Alerts
 - History
 - Summary
 - Histogram (Legacy)
- Notifications
- Event Log

System

Results 1 - 10 of 10 Matching Services

Host	Service	Status	Last Check	Duration	Attempt	Status Information	
localhost	Current Load	OK	12-01-2021 15:02:16	0d 2h 58m 57s	1/4	OK - load average: 0.00, 0.03, 0.05	
	Current Users	OK	12-01-2021 15:02:54	0d 2h 58m 19s	1/4	USERS OK - 2 users currently logged in	
	HTTP	WARNING	12-01-2021 15:01:31	0d 2h 57m 42s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 5179 bytes in 0.002 second response time	
	PING	OK	12-01-2021 15:04:09	0d 2h 57m 4s	1/4	PING OK - Packet loss = 0%, RTA = 0.11 ms	
	Root Partition	OK	12-01-2021 15:04:46	0d 2h 56m 27s	1/4	DISK OK - free space: / 11639 MB (66.91% inode=98%):	
	SSH	OK	12-01-2021 15:05:24	0d 2h 55m 49s	1/4	SSH OK - OpenSSH_7.4 (protocol 2.0)	
	Swap Usage	OK	12-01-2021 15:06:01	0d 2h 55m 12s	1/4	SWAP OK - 52% free (1044 MB out of 2047 MB)	
	Total Processes	OK	12-01-2021 15:01:39	0d 2h 54m 34s	1/4	PROCS OK: 59 processes with STATE = RSZDT	
	web01	HTTPMonitor	CRITICAL	12-01-2021 15:04:29	0d 0h 1m 44s	1/3	(Return code of 255 is out of bounds : (No output on stdout) stderr: connect to address 192.168.169.12 port 5666: Connection refused))
		SSHMonitor	CRITICAL	12-01-2021 15:05:41	0d 0h 0m 32s	1/3	(Return code of 255 is out of bounds : (No output on stdout) stderr: connect to address 192.168.169.12 port 5666: Connection refused))

Mặc định khi mới thêm host, Nagios Server chưa check các dịch vụ. Để check xem dịch vụ trên host có chạy hay không? Chúng ta bấm vào dịch vụ cần check, ở đây tôi sẽ chọn dịch vụ HTTP.

Service Information

Last Updated: Wed Dec 1 15:32:38 +07 2021
 Updated every 90 seconds
 Nagios® Core™ 4.3.1 - www.nagios.org
 Logged in as nagiosadmin

Service
HTTPMonitor
 On Host
My Apache server
 (web01)

General

- [Home](#)
- [Documentation](#)

Current Status

- [Tactical Overview](#)
- [Map \(Legacy\)](#)
- [Hosts](#)
- [Services](#)
- [Host Groups](#)
 - Summary
 - Grid
- [Service Groups](#)
 - Summary
 - Grid
- [Problems](#)
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

- [Availability](#)
- [Trends \(Legacy\)](#)
- [Alerts](#)
 - History
 - Summary
 - Histogram (Legacy)
- [Notifications](#)
- [Event Log](#)

System

- [Comments](#)

Service State Information

Current Status:	CRITICAL (for 0d 0h 28m 9s)
Status Information: (Return code of 255 is out of bounds : (No output on stdout) stderr: connect to address 192.168.169.12 port 5666: Connection refused)	
Performance Data:	
Current Attempt:	3/3 (HARD state)
Last Check Time:	12-01-2021 15:29:34
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.005 seconds
Next Scheduled Check:	12-01-2021 15:39:34
Last State Change:	12-01-2021 15:04:29
Last Notification:	12-01-2021 15:08:29 (notification 1)
Is This Service Flapping?	NO (5.86% state change)
In Scheduled Downtime?	NO
Last Update:	12-01-2021 15:32:34 (0d 0h 0m 4s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

Service Commands

- Disable active checks of this service
- Re-schedule the next check of this service
- Submit passive check result for this service
- Stop accepting passive checks for this service
- Stop obsessing over this service
- Acknowledge this service problem
- Disable notifications for this service
- Delay next service notification
- Send custom service notification
- Schedule downtime for this service
- Disable event handler for this service
- Disable flap detection for this service
- Clear flapping state for this service

3. Tài liệu tham khảo

- [1] Network Monitoring Tools From Nagios : Network Monitoring Tools - Nagios
- [2] <https://github.com/nagios-plugins/nagios-plugins/search?l=perl>
- [3] [meditech-ghichep-nagios/1.Setup-CentOS-7.md at master · meditechopen/meditech-ghichep-nagios · GitHub](https://github.com/meditech-ghichep-nagios/1.Setup-CentOS-7.md)