FTP & SFTP Server Configuration

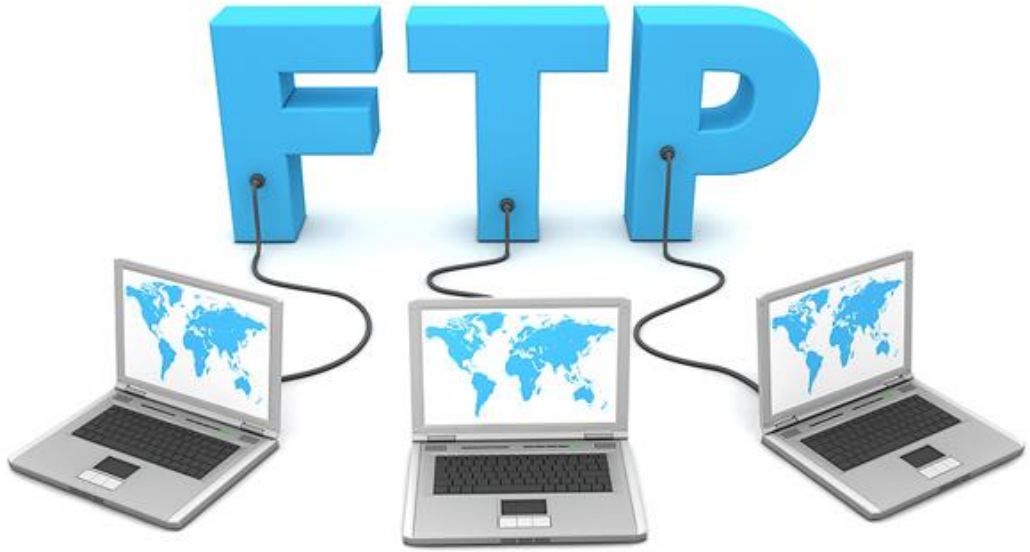
AGENDA

- FTP Server Installation
- FTP Server Configuration
- Allow Firewall Rules
- Access FTP server from window machine
- SFTP Configuration
- Test the connection

FTP Server Installation

Step1: Install FTP server

- yum install vsftpd



FTP Server Installation

```
[root@localhost ~]# yum install vsftpd
Updating Subscription Management repositories.
Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs)                    775  B/s | 4.1 kB     00:05
Red Hat Enterprise Linux 9 for x86_64 - AppStream (RPMs)                 857  B/s | 4.5 kB     00:05
Red Hat Enterprise Linux 9 for x86_64 - AppStream (RPMs)                 3.0 MB/s |  64 MB     00:21
Dependencies resolved.
================================================================================================================================
 Package              Architecture         Version                    Repository                                       Size
================================================================================================================================
Installing:
 vsftpd               x86_64               3.0.5-6.el9                rhel-9-for-x86_64-appstream-rpms                172 k

Transaction Summary
================================================================================================================================
Install  1 Package

Total download size: 172 k
Installed size: 347 k
Is this ok [y/N]: y
Downloading Packages:
vsftpd-3.0.5-6.el9.x86_64.rpm                                            32 kB/s | 172 kB     00:05
--------------------------------------------------------------------------------------------------------------------------------
Total                                                                    32 kB/s | 172 kB     00:05
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                1/1
  Installing       : vsftpd-3.0.5-6.el9.x86_64                                                      1/1
  Running scriptlet: vsftpd-3.0.5-6.el9.x86_64                                                      1/1
  Verifying        : vsftpd-3.0.5-6.el9.x86_64                                                      1/1
Installed products updated.

Installed:
  vsftpd-3.0.5-6.el9.x86_64

Complete!
[root@localhost ~]# _
```

FTP Server Configuration

Step2: Edit vsftpd.conf

❖ Take Backup of the existing config file\

- mv /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.bak

❖ Create new config file

- vi /etc/vsftpd/vsftpd.conf

FTP Server Configuration

- Take Backup of existing configuration file

```
[root@localhost ~]# cd /etc/vsftpd/
[root@localhost vsftpd]# mv /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.bak
[root@localhost vsftpd]# ll
total 20
-rw-------. 1 root root  125 Aug 20  2024 ftpusers
-rw-------. 1 root root  361 Aug 20  2024 user_list
-rw-------. 1 root root 5039 Aug 20  2024 vsftpd.conf.bak
-rwxr--r--. 1 root root  352 Aug 20  2024 vsftpd_conf_migrate.sh
[root@localhost vsftpd]# _
```

FTP Server Configuration

Enable the following parameters in the config file

anonymous_enable=NO	Disables anonymous FTP access, ensuring that only authenticated users with valid credentials can access the FTP server
local_enable=YES	Allow local users with system accounts to log in to the FTP server
write_enable=YES	Enables write permission for authenticated users, allowing them to upload files to the FTP server
local_umask=022	Sets the default permissions for uploaded files by local users to 644 and directories to 755
dirmessage_enable=YES	Enables the display of directory messages, which are files named .message within directories that contain a message to be displayed to users upon entering the directory
xferlog_enable=YES	Enables logging of FTP file transfers, which can be useful for monitoring and auditing purposes.

FTP Server Configuration

Enable the following parameters in the config file

connect_from_port_20=YES	Specifies that data connections should originate from port 20, which is the traditional FTP data transfer port.
xferlog_std_format=YES	Sets the logging format to standard format for better compatibility with FTP log analyzers
listen=NO	Disables standalone mode, allowing VSFTP to run as a service managed by systemd
listen_ipv6=YES	Enables listening on IPv6 addresses in addition to IPv4 addresses
pam_service_name=vsftpd	Specifies the PAM service name used for authentication

FTP Server Configuration

Enable the following parameters in the config file

pasv_enable=YES	Enables passive mode, allowing clients to initiate data connections to the FTP server.
pasv_min_port=30000	Specifies the range of passive ports to be used for data connections.
pasv_max_port=31000	Specifies the range of passive ports to be used for data connections.
userlist_enable=YES	Enables the use of a user list for access control.
userlist_file=/etc/vsftpd.userlist	Specifies the file where the list of allowed users is stored.

FTP Server Configuration

Enable the following parameters in the config file

userlist_deny=NO	Specifies that users listed in userlist_file are allowed to access the FTP server
chroot_local_user=YES	Places local users in a chroot jail, restricting their access to their home directory after login
user_sub_token=$USER	Substitutes $USER with the actual username, allowing each user to have their own directory
local_root=/home/$USER/ftp	Sets the local root directory for each user to their respective home directory under /home, ensuring that each user is chrooted to their own directory upon login

FTP Server Configuration

```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# 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.
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.
# When SELinux is enforcing check for SE bool allow_ftpd_anon_write, allow_ftpd_full_access
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
```

FTP Server Configuration

```
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/xferlog
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode. The vsftpd.conf(5) man page explains
# the behaviour when these options are disabled.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
```

FTP Server Configuration

```
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES

userlist_file=/etc/vsftpd/user_list
userlist_deny=NO

pam_service_name=vsftpd
userlist_enable=YES


chroot_local_user=YES
allow_writeable_chroot=YES
user_sub_token=$USER
local_root=/home/$USER/
```

FTP Server Services

Step3: Start/restart FTP Service

❖ Enable the service

- systemctl enable vsftpd.service

❖ Start/restart the service

- systemctl start/restart vsftpd.service

FTP Server Services

```
[root@localhost vsftpd]# systemctl enable vsftpd.service
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
[root@localhost vsftpd]# systemctl start vsftpd.service
[root@localhost vsftpd]# systemctl status vsftpd.service
● vsftpd.service - Vsftpd ftp daemon
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: disabled)
     Active: active (running) since Thu 2025-07-24 20:09:22 +08; 27s ago
    Process: 5455 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
   Main PID: 5456 (vsftpd)
      Tasks: 1 (limit: 10527)
     Memory: 1.1M
        CPU: 7ms
     CGroup: /system.slice/vsftpd.service
             └─5456 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Jul 24 20:09:22 localhost.localdomain systemd[1]: Starting Vsftpd ftp daemon...
Jul 24 20:09:22 localhost.localdomain systemd[1]: Started Vsftpd ftp daemon.
[root@localhost vsftpd]# _
```

Allow Firewall Rules

Step 4: Add FTP port and service in the Firewall

❖ Add the FTP port

- firewall-cmd --add-port=20-21/tcp --permanent

❖ Add Passive port

- firewall-cmd --add-port=30000-31000/tc --permanent

Allow Firewall Rules

Step 4: Add FTP port and service in the Firewall

- Add FTP service
  - firewall-cmd –add-service=ftp --permanent
- Reload firewall
  - firewall-cmd --reload

FTP Server Services

```
[root@localhost vsftpd]# firewall-cmd --add-port=20-21/tcp --permanent
success
[root@localhost vsftpd]# firewall-cmd --add-port=30000-31000/tcp --permanent
success
[root@localhost vsftpd]# firewall-cmd --add-service=ftp --permanent
success
[root@localhost vsftpd]# firewall-cmd --reload
success
[root@localhost vsftpd]# _
```

FTP User and Access

Step 5: Create FTP User and add to user list

❖ Create User

- useradd ftp_satthya
- chown root:root /home/ftp_satthya
- chmod 755 /home/ftp_satthya

- mkdir –p /home/ftp_satthya/ftp
- chown ftp_satthya:ftp_satthya /home/ftp_satthya/ftp

❖ Update user_list

- vi /etc/vsftpd/user_list

FTP Server Services

```
[root@localhost ~]# useradd ftp_satthya
[root@localhost ~]# chown root:root /home/ftp_satthya/
[root@localhost ~]# chmod 755 /home/ftp_satthya/
[root@localhost ~]# mkdir-p /home/ftp_satthya/ftp
-bash: mkdir-p: command not found
[root@localhost ~]# mkdir -p /home/ftp_satthya/ftp
[root@localhost ~]# chown ftp_satthya:ftp_satthya /home/ftp_satthya/ftp/
[root@localhost ~]# cd /home/ftp_satthya/
[root@localhost ftp_satthya]# ll
total 0
drwxr-xr-x. 2 ftp_satthya ftp_satthya 6 Jul 25 12:16 ftp
[root@localhost ftp_satthya]#
```

FTP Server Services

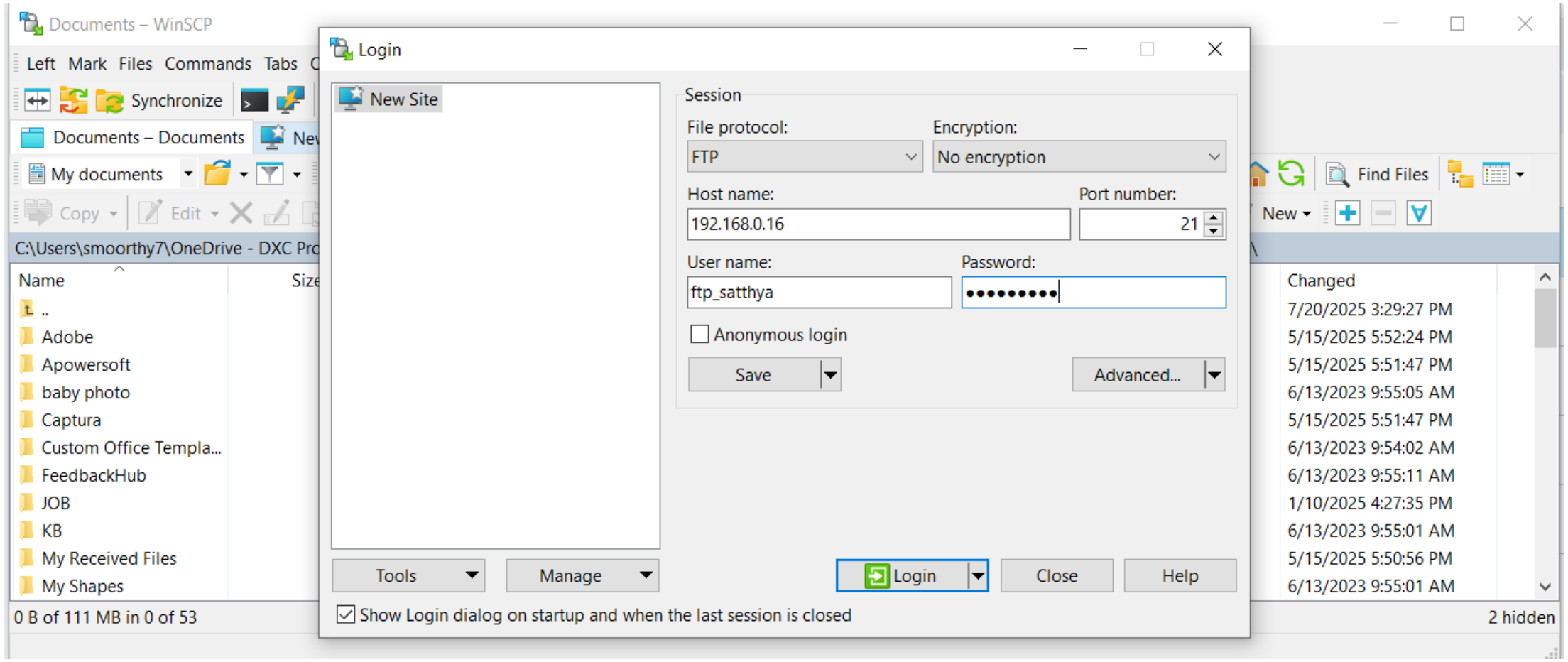
```
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon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

Access FTP server from window machine

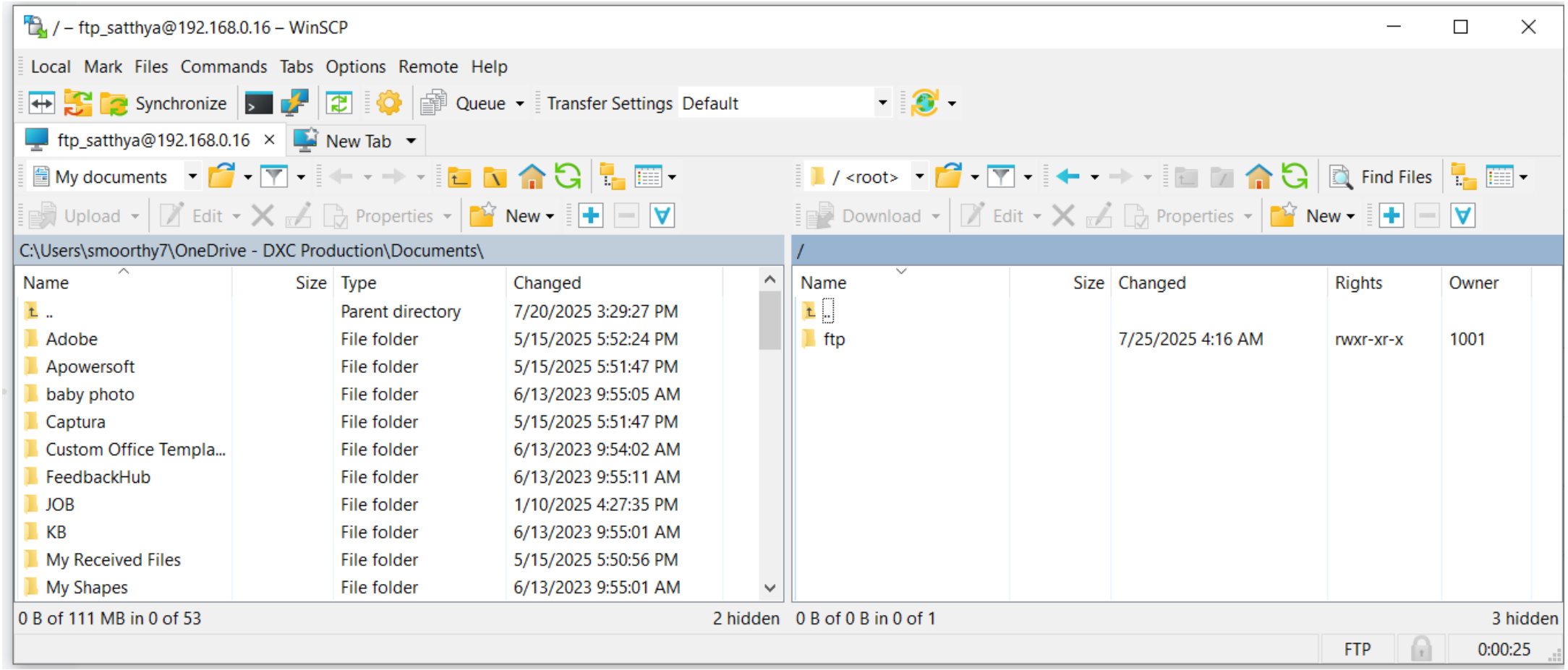
Step 6: Access FTP server using winSCP

- File Protocol : FTP
- Host Name : FTP Server IP Address
- User Name : FTP username
- Password : FTP user password

FTP Server Services



FTP Server Services



SFTP Configuration

Step 7 : Configure SFTP to prevent user from ssh

❖ Install SSH

- yum install openssh-server

❖ Edit SSH config file

- vi /etc/ssh/sshd_config

SFTP Configuration

- Update below parameters in sshd config file :
  - Match User ftp_satthya
    - ForceCommand internal-sftp
    - PasswordAuthentication yes
    - ChrootDirectory /home/ftp_satthya
    - PermitTunnel no
    - AllowAgentForwarding no
    - X11Forwarding no

SFTP Configuration

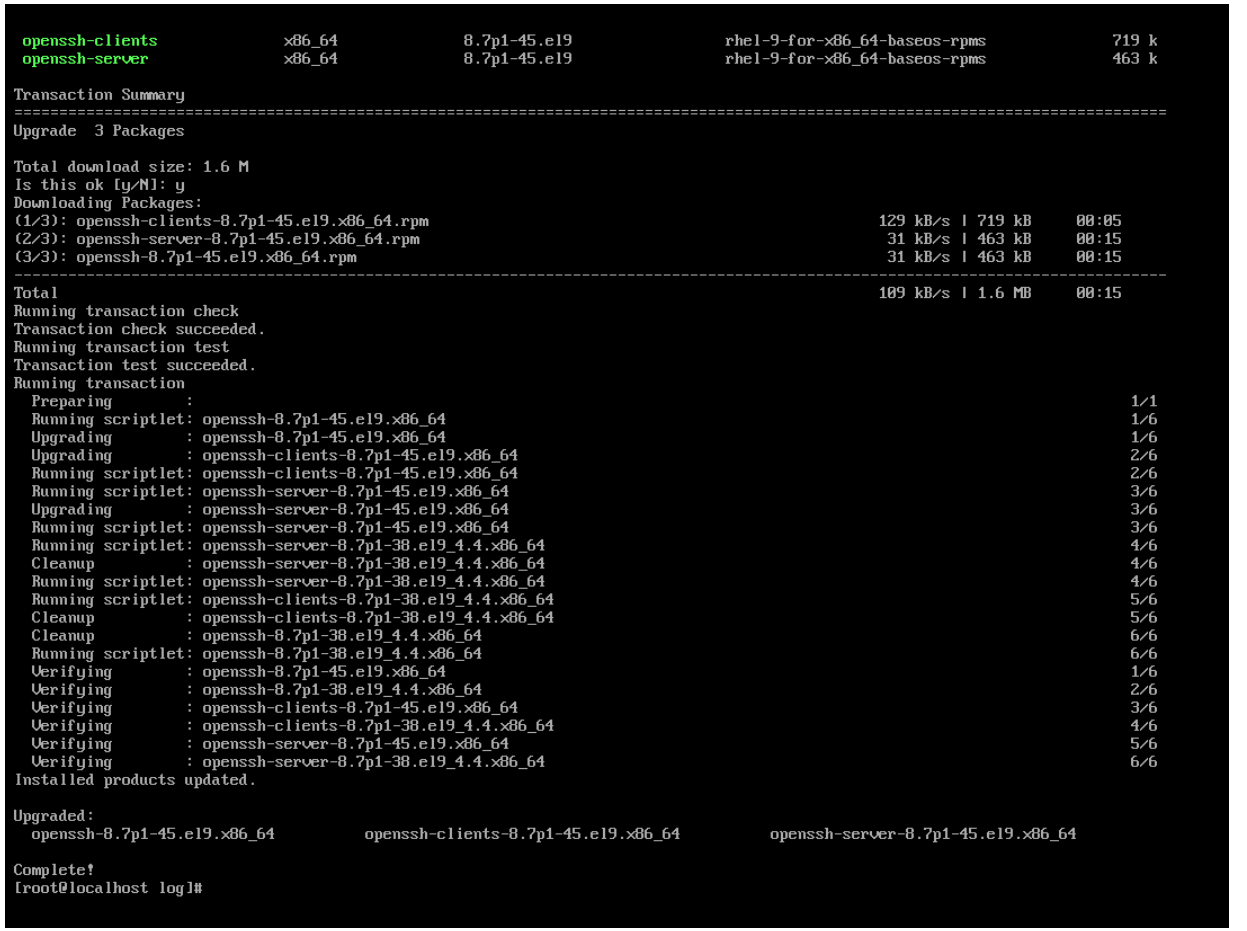
Step 8 : Restart ssh service

❖ systemctl restart sshd

Remark : After enabling SFTP with chroot configuration, the ftpuser will be restricted to the specified directory (e.g., /home/ftp_satthya) and will not have SSH shell access. Only SFTP file transfers are allowed.

SFTP Configuration

- OPEN-SSH INSTALLATION



SFTP Configuration

- Edit SSH config file

```
# and KbdInteractiveAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in RHEL and may cause several
# problems.
#UsePAM no

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

Match User ftp_satthya
 ForceCommand internal-sftp
 PasswordAuthentication yes
 ChrootDirectory /home/ftp_satthya
 PermitTunnel no
 AllowAgentForwarding no
 X11Forwarding no

-- INSERT --
```

FTP Connection Troubleshooting – Server Side

- ❖ Check vsftpd service status
- ❖ Check firewall setting
- ❖ Verify if port 21 is listening
- ❖ Check vsftpd config file for errors
- ❖ Verify user is allowed in userlist
- ❖ Check user’s home directory and permissions
- ❖ Check for passive mode ports
- ❖ Check logs for error

END