CONFIGURATION OF SFTP IN UBUNTU SERVER

1. LOGIN IN TO THE MACHINE AS ROOT USER
   Sudo -i

2. THEN WE NEED TO UPDATE THE SYSTEM FILES
   Sudo apt update
   Sudo apt upgrade

3. WE NEED TO INSTALL THE SSH
   Sudo apt install ssh
   Sudo systemctl enable ssh
   Sudo systemctl start ssh
   Sudo systemctl status ssh - to check for active state.

4. THEN WE NEED TO ADD GROUPS AND USERS
   Sudo addgroup sftp (any name)
   The group created with the name of sftp.
   Sudo adduser test (any name)
   The user was created with the name of test.

```
root@IXLAP71:~# sudo addgroup ftp
Adding group `ftp' (GID 1002) ...
Done.
root@IXLAP71:~# sudo adduser test
Adding user `test' ...
Adding new group `test' (1003) ...
Adding new user `test' (1001) with group `test' ...
Creating home directory `/home/test' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
Enter the new value, or press ENTER for the default
        Full Name []: test
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

   Create new password for that test user.

CONFIGURATION OF SFTP IN UBUNTU SERVER

5. **Sudo usermod -a -G sftp test (Adding the user test in to sftp group by this command)**

- **`sudo`**: This command allows you to execute another command as a superuser or another user, typically with administrative privileges. It's often used to perform actions that require higher permissions.
- **`usermod`**: This command is used to modify user account properties in Unix-like operating systems.
- **`-a`**: This option specifies that you want to add the user to a group without removing them from any other groups.
- **`-G sftp`**: This option indicates the name of the group to which you want to add the user. In this case, it's the "sftp" group.
- **`test`**: This is the username of the user you want to add to the "sftp" group.

6. **grep sftp /etc/group**
   sftp:x:1001:test (we need to get this as output by executing above command)

- **`sftp`**: This is the name of the group.
- **`x`**: This field typically represents the group's password, but it's usually set to "x" (indicating that an encrypted password is stored elsewhere or that no password is set).
- **`1001`**: This is the group's numerical ID (GID).
- **`test`**: This is a list of usernames that are part of the "sftp" group. In this case, it indicates that the user "test" is a member of the "sftp" group.

So, this output indicates that the "sftp" group exists on your system, and the user "test" is a member of this group. This setup allows the user "test" to potentially have access to SFTP services and any permissions associated with the "sftp" group, depending on your system's configuration.

CONFIGURATION OF SFTP IN UBUNTU SERVER

7. Now we need to create a particular directory to the user can access its content only.
   Sudo mkdir -p /home/test(any user name)/files/

- `mkdir`: This is the command used to create directories (folders) on the filesystem.
- `-p`: This option is used to ensure that parent directories are created as needed. If any of the parent directories in the given path do not exist, they will be created.

8. Giving ownership to the directory for the root user
   Sudo chown root:root /home/test(any user name)
   Sudo chmod 755 /home/test(any user name)

- `chmod`: This command is used to change the permissions of files and directories.

- `755`: This is a numeric representation of the permissions you want to apply to a file or directory. Each digit represents a different permission set:
  - The first digit (7) represents the owner's permission. In this case, it's read, write, and execute (4 + 2 + 1 = 7).
  - The second digit (5) represents the group's permission, which is read and execute (4 + 1 = 5).
  - The third digit (5) represents others' (everyone else's) permission, which is also read and execute.

When combined, `755` gives the owner full permissions (read, write, and execute), and groups and others have read and execute permissions. This is a common permission setting for executable files and directories.

9. Giving permission to the user for particular paths and files.
   Sudo chown test:test /home/test/files

CONFIGURATION OF SFTP IN UBUNTU SERVER

10. Changing configuration files to adding user
    Sudo nano /etc/ssh/sshd_config

    Add these lines in the end of the config file then save and exit nano.

    Match User test
    ChrootDirectory /home/test/files
    X11Forwarding no
    AllowTcpForwarding no
    Forcecommand internal-sftp

    This means that when an SFTP user named "test" logs in, they will be confined to the directory **`/home/test/files`**. They won't be able to navigate beyond this directory in their SFTP sessions.

11. Now we need to restart the ssh to take the effect.
    sudo systemctl restart ssh

12. To know the connection ip we need to enter
    Ifconfig

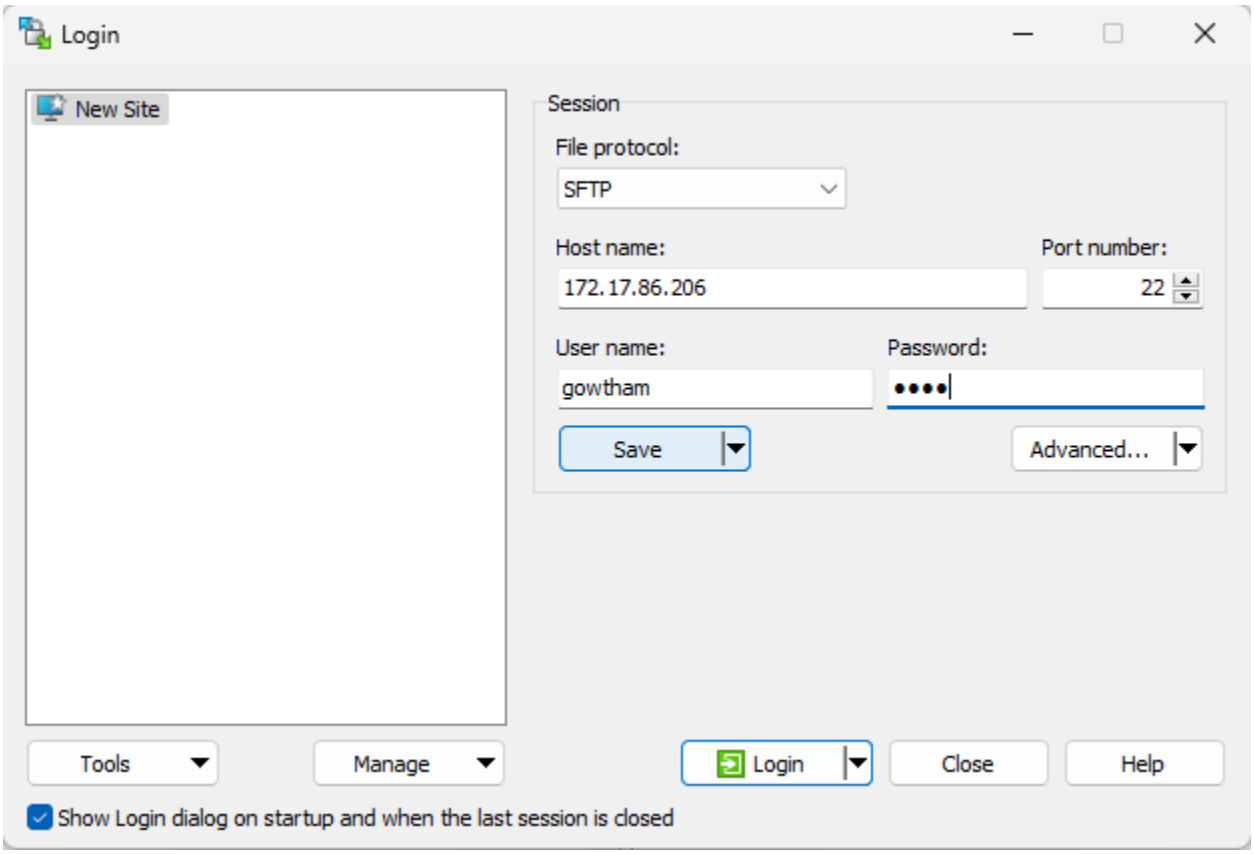
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.86.206  netmask 255.255.240.0  broadcast 172.17.95.255
        inet6 fe80::215:5dff:fee7:516b  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:e7:51:6b  txqueuelen 1000  (Ethernet)
        RX packets 1752  bytes 636222 (636.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 310  bytes 85229 (85.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

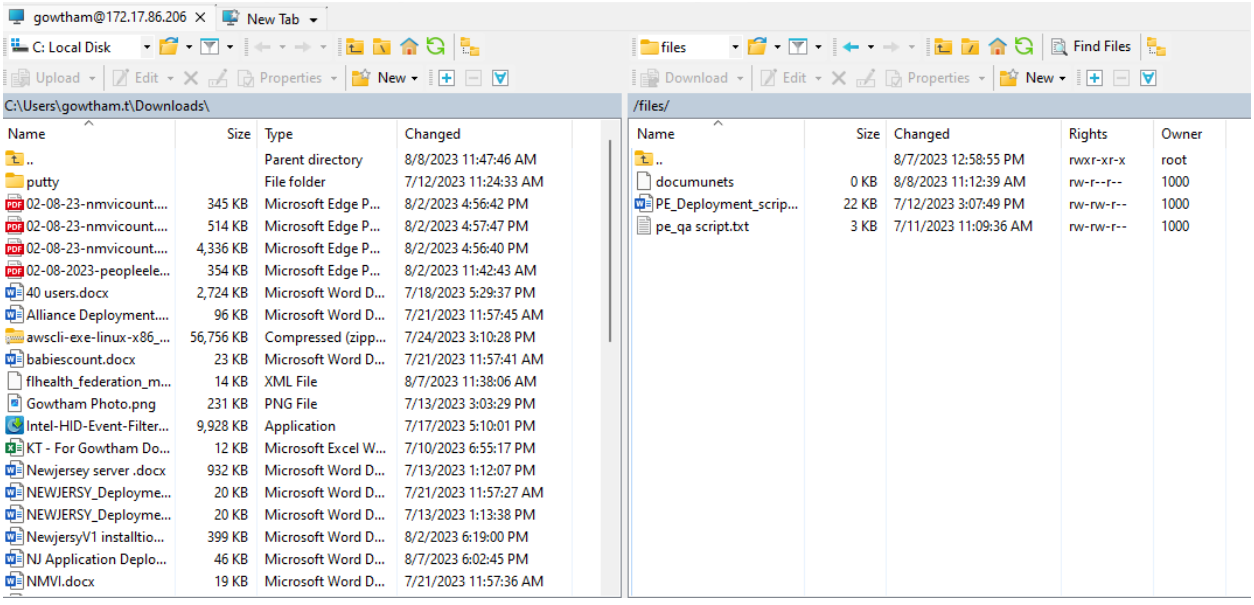
To login winscp need the ip from inlet 172.17.86.206

And enter the username we create

Type password to login winscp to files transfer to particular path.

CONFIGURATION OF SFTP IN UBUNTU SERVER





User can access the particular files path /home/test/files