

FTP/SFTP Server Configuration

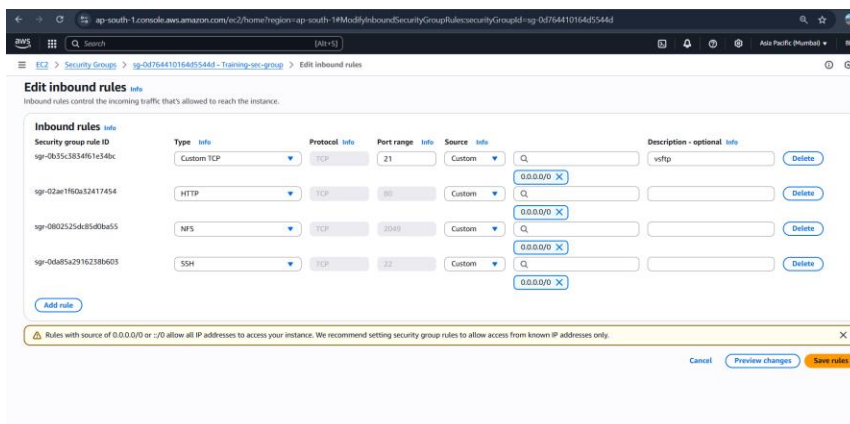
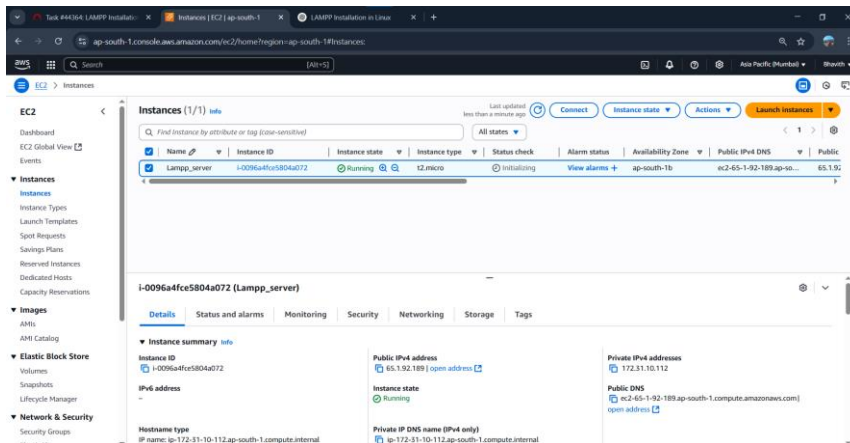
Goal

Enable file transaction to servers using File Transfer Protocol (FTP).

Step 1: Launch AWS EC2 Instance

1. Launch an Amazon Linux 2 EC2 instance.
2. Allow inbound ports 22 and 21 in the security group.
3. Connect to the instance using Git Bash:

```
ssh -i "your-key.pem" ec2-user@your-ec2-public-ip
```

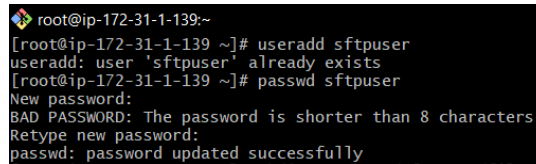


Step 2: Configure SFTP on Port 22

1. Create a new user:

```
sudo adduser sftpuser
```

```
sudo passwd sftpuser
```

A terminal window with a black background and white text. The prompt is root@ip-172-31-1-139:~. The user runs 'useradd sftpuser' and receives the message 'useradd: user 'sftpuser' already exists'. Then they run 'passwd sftpuser' and are prompted for a new password. They enter a password, but it's rejected with 'BAD PASSWORD: The password is shorter than 8 characters'. They retype a longer password, and it's accepted with the message 'passwd: password updated successfully'.

```
root@ip-172-31-1-139:~  
[root@ip-172-31-1-139 ~]# useradd sftpuser  
useradd: user 'sftpuser' already exists  
[root@ip-172-31-1-139 ~]# passwd sftpuser  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully
```

2. Create a directory and set permissions:

```
sudo mkdir -p /home/sftpuser/files
```

```
sudo chown root:root /home/sftpuser
```

```
sudo chmod 755 /home/sftpuser
```

```
sudo chown sftpuser:sftpuser /home/sftpuser/files
```

A terminal window with a black background and white text. The prompt is ec2-user@ip-172-31-24-53 ~ (git:master). The user runs 'mkdir -p /home/sftpuser/home/sftpuser/files', 'chown root:root /home/sftpuser', 'chmod 755 /home/sftpuser', and 'chown sftpuser:sftpuser /home/sftpuser/files'.

```
EC2AMAZ-FH150FF_AN:ec2-user@ip-172-31-24-53 ~ (git:master) →  
ec2-user@ip-172-31-24-53 ~(git:master)  
ec2-user:sudo mkdir -p /home/sftpuser/home/sftpuser/files  
ec2-user:sudo chown root:root /home/sftpuser  
ec2-user:sudo chmod 755 /home/sftpuser  
ec2-user:sudo chown sftpuser:sftpuser /home/sftpuser/files
```

3. Edit SSH config:

```
sudo vim /etc/ssh/sshd-custom_config
```

Add at end:

```
Match User sftpuser
```

```
ChrootDirectory /home/sftpuser
```

```
ForceCommand internal-sftp
```

```
AllowTcpForwarding no
```

2. Create a new user:

```
sudo adduser ftpuser
sudo passwd ftpuser
```

```
[root@ip-172-31-1-139 ~]# useradd ftpuser
[root@ip-172-31-1-139 ~]# passwd ftpuser
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
[root@ip-172-31-1-139 ~]#
```

3. Create and set permissions for directory:

```
sudo mkdir -p /home/ftpuser/ftpfiles
sudo chown nobody:nobody /home/ftpuser
sudo chmod a-w /home/ftpuser
sudo chown ftpuser:ftpuser /home/ftpuser/ftpfiles
```

```
[root@ip-172-31-1-139 ~]# mkdir -p /home/ftpuser/ftpfiles
[root@ip-172-31-1-139 ~]# chown ftpuser:ftpuser /home/ftpuser/ftpfiles
[root@ip-172-31-1-139 ~]# cp /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.bak
[root@ip-172-31-1-139 ~]#
```

4. Configure vsftpd:

```
sudo vim /etc/vsftpd/vsftpd-custom.conf
```

Ensure the following:

anonymous_enable=NO

local_enable=YES

```
write_enable=YES
```

```
chroot_local_user=YES
```

pasv_min_port=10000

pasv_max_port=10100

```
user_sub_token=$USER
```

```
local_root=/home/$USER/ftp
```

[illegible]

5. Enable passive ports in security group (10000-10100)

training-sec-group		1 rule
Type	Protocol	Source
Custom TCP	10000-10100	0.0.0.0/0

6. Restart vsftpd:

```
sudo systemctl start vsftpd  
sudo systemctl enable vsftpd
```

7. Verify using Cyberduck (Protocol: FTP, Port: 21)

