# How to Set Up SFTP Chroot Jail

Posted Apr 7, 2019 • 5 min read

RELATED TUTORIALS

How to Change the SFTP Port

How to Set up SSH Tunneling (Port Forwarding)

How to use SSHFS to Mount Remote Directories over SSH

Generate SSH Keys on Windows with PuTTYgen

How to Change the SSH Port in Linux

How to Set Up SSH Keys on Ubuntu 20.04

How to Set Up SSH Keys on CentOS 8

If you are a system administrator managing Linux server chances are that you may need to grant SFTP access to some users to upload files to their home directories. By default, users that can log in to the system via SSH, SFTP and SCP can browse the entire filesystem including other user's directories. This may not be a problem if these users are trusted, but if you don't want the logged in users to navigate around the system you will need to restrict user access to their home directory. This adds an extra layer of security especially on systems with multiple users.

In this tutorial, we will explain how to setup up an SFTP Chroot Jail environment that will restrict users to their home directories. The users will have SFTP access only, SSH access will be disabled. These instructions should work for any modern Linux distribution including Ubuntu, CentOS, Debian, and Fedora.

## Creating an SFTP Group

Instead of configuring the OpenSSH server for each user individually we will create a new group and add all our chrooted users to this group.

Run the following `groupadd` command to create the `sftponly` user group:

```
$ sudo groupadd sftponly
```

> You can name the group as you want.

## Adding Users to the SFTP Group

The next step is to add the users you want to restrict to the `sftponly` group.

If this is a new setup and the user doesn’t exist you can create a new user account by typing:

```
$ sudo useradd -g sftponly -s /bin/false -m -d /home/username username
```

- The `-g sftponly` option will add the user to the sftponly group.

- The `-s /bin/false` option sets the user's login shell. By setting the login shell to `/bin/false` the user will not be able to login to the server via SSH.
- The `-m -d /home/username` options tells useradd to create the user home directory.

Set a strong password for the newly created user:

```
$ sudo passwd username
```

Otherwise if the user you want to restrict already exist, add the user to the `sftponly` group and change the user's shell:

```
$ sudo usermod -G sftponly -s /bin/false username2
```

The user home directory must be owned by root and have `755` permissions :

```
$ sudo chown root: /home/username
$ sudo chmod 755 /home/username
```

Since the users home directories are owned by the root user, these users will no be able to create files and directories in their home directories. If there are no directories in the user's home, you'll need to create new directories to which the user will have full access. For example, you can create the following directories:

```
$ sudo mkdir /home/username/{public_html,uploads}
$ sudo chmod 755 /home/username/{public_html,uploads}
$ sudo chown username:sftponly /home/username/{public_html,uploads}
```

If a web application is using the user's `public_html` directory as document root, these changes may lead to permissions issues. For example, if you are running WordPress you will need to create a PHP pool that will run as the user owning the files and add the webs erver to the `sftponly` group.

## Configuring SSH

SFTP is a subsystem of SSH and supports all SSH authentication mechanisms.

Open the SSH configuration file `/etc/ssh/sshd_config` with your text editor :

```
$ sudo nano /etc/ssh/sshd_config
```

Search for the line starting with `Subsystem sftp`, usually at the end of the file. If the line starts with a hash `#` remove the hash `#` and modify it to look like the following:

/etc/ssh/sshd_config

```
Subsystem sftp internal-sftp
```

Towards the end of the file, the following block of settings:

/etc/ssh/sshd_config

```
Match Group sftponly
  ChrootDirectory %h
  ForceCommand internal-sftp
  AllowTcpForwarding no
  X11Forwarding no
```

The `ChrootDirectory` directive specifies the path to the chroot directory. `%h` means the user home directory. This directory, must be owned by the root user and not writable by any other user or group.

Be extra careful when modifying the SSH configuration file. The incorrect configuration may cause the SSH service to fail to start.

Once you are done save the file and restart the SSH service to apply the changes:

```
$ sudo systemctl restart ssh
```

In CentOS and Fedora the ssh service is named `sshd` :

```
$ sudo systemctl restart sshd
```

## Testing the Configuration

Now that you have configured SFTP chroot you can try to login to the remote machine through SFTP using the credentials of the chrooted user. In most cases, you will use a desktop SFTP client like FileZilla but in this example, we will use the sftp command .

Open an SFTP connection using the sftp command followed by the remote server username and the server IP address or domain name:

```
$ sftp username@192.168.121.30
```

You will be prompted to enter the user password. Once connected, the remote server will display a confirmation message and the `sftp>` prompt:

Output

```
username@192.168.121.30's password:
sftp>
```

Run the `pwd` command, as shown below, and if everything is working as expected the command should return `/`.

Output

```
sftp> pwd
Remote working directory: /
```

You can also list the remote files and directories using the `ls` command and you should see the directories that we have previously created:

Output

```
sftp> ls
public_html  uploads
```

## Conclusion

In this tutorial, you have learned how to setup up an SFTP Chroot Jail environment on your Linux server and restrict user access to their home directory.

By default, SSH listens on port 22. Changing the default SSH port adds an extra layer of security to your server by reducing the risk of automated attacks. You may also want to set up an SSH key-based authentication and connect to the server without entering a password.

If you have any questions or feedback, feel free to leave a comment.

ssh sftp security

## Related Articles

JUL 24, 2020

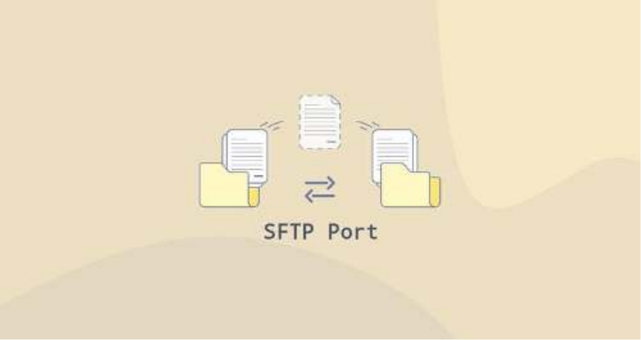
How to Change the SFTP Port

AUG 8, 2019

How to Set up SSH Tunneling (Port Forwarding)

MAY 12, 2019

How to use SSHFS to Mount Remote Directories over SSH



Show comments (3)