# SFTP Server Setup

This playbook outlines the steps required to configure a secure SFTP server. It is designed to ensure encrypted file transfers within a network, enhancing security and data integrity.

### Step 1: Prerequisites

Before beginning the setup, ensure the following requirements are met: a server with internet access, SSH installed, and root or sudo privileges.

### Step 2: Install SFTP

Install the SFTP server software on the machine that will serve as the SFTP server.

### Step 3: Configure SSH

Edit the SSH daemon configuration file '/etc/ssh/sshd\_config' to enable an SFTP subsystem and define security and access parameters.

### Step 4: Create Users

Create user accounts on the server that will be used specifically for SFTP, with restricted access to their home directories only.

### Step 5: Set Permissions

Adjust the file and directory permissions to secure the data and ensure that users only have access to their respective directories.

### Step 6: Restart SSH

Restart the SSH service to apply the new configuration settings.

### Step 7: Verify Setup

Test the SFTP connection using an SFTP client to ensure that everything is configured correctly and that file transfers are securely facilitated.

## General Notes

### SSH Keys

For additional security, consider setting up SSH key-based authentication for the users instead of password-based authentication.

### Firewall

Make sure to configure the server's firewall to allow SFTP connections, typically over port 22.

### Backups

Regularly backup the server and SFTP user data to prevent loss in the event of a failure or breach.