Is there solution to show users only desired folders as they can see all other folders while using SFTP?

439 Riya Francis January 21, 2025 Common Errors & Troubleshooting, General 6099

Restricting SFTP User Access to Specific Folders in gateway server

Overview: This article addresses how to restrict SFTP users to only view specific folders in gateway server, noting that due to system restrictions, chroot cannot be applied through ezeelogin itself, and SSHD must be used instead.

Unfortunately, the chroot doesn't work due to system restrictions as the Ezsh (Ezeelogin shell) works as a non-privileged user. The only option would be to rely on SSHD to do the chroot.

Example: Configuring SSHD for Chroot

Step 1: Edit the SSHD Configuration File:

Open the SSHD configuration file (/etc/ssh/sshd_config) in a text editor.

```
root@gateway:~# nano /etc/ssh/sshd_config
```

Step 2: Add Chroot Configuration:

Add the following lines to the configuration file to set up a chroot jail for a specific user or group. In this example, we'll restrict SFTP access for a user named sftpuser:

```
Match User sftpuser
ChrootDirectory /home/sftpuser
ForceCommand internal-sftp
AllowTcpForwarding no
X11Forwarding no
```

Match User sftpuser: Applies the following settings only to sftpuser.
ChrootDirectory /home/sftpuser: Sets the chroot directory to /home/sftpuser.
ForceCommand internal-sftp: Forces the use of the internal SFTP server.
AllowTcpForwarding no: Disables TCP forwarding for the user.
X11 Forwarding: Disables X11 forwarding.

Step 3: Set Proper Permissions:

Ensure that the chroot directory and its parent directories have the correct permissions.

For example:

```
root@gateway:~# sudo chown root:root /home/sftpuser
root@gateway:~# sudo chmod 755 /home/sftpuser
root@gateway:~# sudo mkdir /home/sftpuser/uploads
root@gateway:~# sudo chown sftpuser:sftpuser /home/sftpuser/uploads
```

The root directory of the chroot jail must be owned by the root and have 755 permissions.
Subdirectories, such as uploads, can be owned by the user.

Step 4: Restart SSHD:

Apply the configuration changes by restarting the SSHD service:

```
root@gateway:~# systemctl restart sshd
```

Step 5: Verify Access Restrictions:

Test the SFTP connection as sftpuser to confirm that the user is confined to the /uploads directory and cannot access other parts of the filesystem.

After logging in, the user should only see and interact with files within the /uploads directory.

Related Articles:

Restrict SFTP connections to specific ports.

Online URL: https://www.ezeelogin.com/kb/article/is-there-solution-to-show-users-only-desired-folders-as-they-can-see-all-other-folders-while-using-sftp-439.html