Configuring SFTP on a Windows Server

**Background**

This document explains how to setup SFTP on a windows server box. It can be done on a wincore box as well as all the operations are command line driven.

**Config details for TS and Test Rigs in Lab Manager**

**SFTP Server:**

TS-WINSFTP1 on Port 22

Service Name: sshd Password: Pa55word

**SFTP Users:**

|  |  |  |
| --- | --- | --- |
| **Username** | **Password** | **Windows File Share\*** |
| SFTPClient1 | Test1234 | [\\ts-winsftp1\SFTPClient1](file:///\\ts-winsftp1\SFTPClient1) |
| SFTPClient2 | Test1234 | [\\ts-winsftp1\SFTPClient2](file:///\\ts-winsftp1\SFTPClient2) |

\*The Windows file share provides windows access to the files available through SFTP.

**Setting up SFTP server**

This is done by using cygwin. You can look at an existing rig to see the configuration.

First install OpenSSH using Cygwin based on the following instruction guides:-

<http://www.howtogeek.com/howto/41560/how-to-get-ssh-command-line-access-to-windows-7-using-cygwin/>

<http://code.google.com/p/soi-toolkit/wiki/InstallationGuideCygwinSetup>

Here are the overall steps:-

1. Copy Install folder from [\\onelondon.tfl.local\shared\4723\Systems Development and Delivery\11 - Software Solutions\112 - Development\1121 - Resources\cygwin\cygwin.sftp.install](file:///\\onelondon.tfl.local\shared\4723\Systems%20Development%20and%20Delivery\11%20-%20Software%20Solutions\112%20-%20Development\1121%20-%20Resources\cygwin\cygwin.sftp.install) to d:\Media\cygwin.install
2. Install to d:\cygwin (see guides for instructions)
3. After the ssh-host-config step create the following LOCAL users:-
   1. SFTPClient1 Test1234
   2. SFTPClient2  Test1234
4. Use the following to create a passwd file:-  
   mkpasswd.exe -l >>../etc/passwd
5. Edit the passwd file to set the home folders of the SFTPClient\* accounts to d:\tfl\sharedfolders\SFTPClient\*

It should look something like

SFTPClient1:unused:1013:513:SFTPClient1,U-TS-WINSFTP1\SFTPClient1,S-1-5-21-2495840640-110752177-577786008-1013:/cygdrive/d/tfl/sharedfolders/SFTPClient1:/bin/bash

1. Share the folders d:\tfl\sharedfolders\SFTPClient\* as SFTPClient\*
2. Stop and start the windows service ‘CYGWIN sshd’ to give the service account ‘log on as service rights, make sure it is setup to automatic startup
3. Test connections using

$ sftp SFTPClient2@ts-winsftp1

$ ls

**Creating and Configuring a Public Private Key Pair for SFTP Authentication**

See http://www.debuntu.org/secure-your-ssh-server-with-publicprivate-key-authentification/

1. Log onto the SFTP server and open the cygwin shell.
2. Type to create a key pair. 'PassPhrase' is used to encrypt the private key when it is sent to the server, it be left blank, in which case the private key is not encrypted on transmission
3. *user@host$ ssh-keygen  
   Generating public/private rsa key pair.  
   Enter file in which to save the key (/home/user/.ssh/id\_rsa):  
   Enter passphrase (empty for no passphrase):  
   Enter same passphrase again:  
   Your identification has been saved in /home/user/.ssh/id\_rsa.  
   Your public key has been saved in /home/user/.ssh/id\_rsa.pub.  
   The key fingerprint is:  
   XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX user@host*
4. The above works for ssh2. for ssh1 *use* **ssh-keygen -t rsa1**
5. id\_rsa is the private key and must be made available to the client by copying onto the client machine
6. Now we must configure the public key for a SFTP user, there are two ways to do this

**Configure the server using cygwin cmd lines**

1. Copy the public key the SFTP users working dir on the server
2. *tfsbuild@ts-winsftp1:~$ scp ~/.ssh/id\_rsa.pub SFTPClient1@ ts-winsftp1:~/*
3. Connect as the SFTP user and add the public key to the authorized keys file
4. *$ ssh SFTPClient1@ ts-winsftp1  
   SFTPUser1@ ts-winsftp1password:  
   SFTPUser1@ ts-winsftp1:~$ cat id\_rsa.pub >> ~/.ssh/authorized\_keys  
   SFTPUser1@ ts-winsftp1:~$ rm id\_rsa.pub  
   SFTPUser1@ ts-winsftp1:~$ exit*

**Configure the server by manually copying files**

1. Create a folder named .ssh in the SFTP users working folder (.ssh is not a valid windows folder name so you cannot use windows explorer to do that, use mkdir instead)
2. Copy the public key file into the .ssh folder
3. Rename the file to 'authorized\_keys'

**Check Key Authentication is Enabled**

1. Go to /etc/sshd\_config and check the following are enabled

*RSAAuthentication yes  
 PubkeyAuthentication yes*

**Testing Key Authentication**

Use: ssh SFTPClient1@ts-winsftp1 -i /path/to/private/key