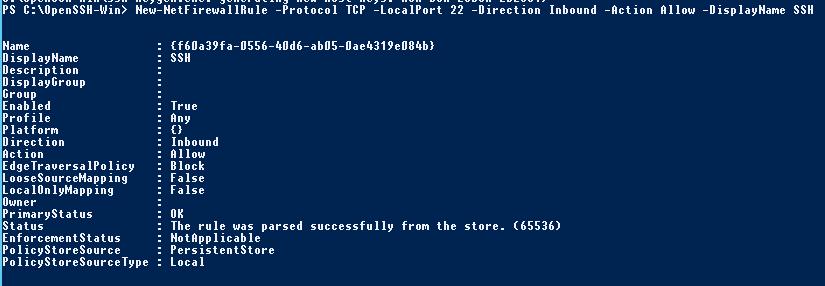
Installation of Win64 OpenSSH on Windows Server 2012 R2

You can download a compiled version of the package here: [https://github.com/PowerShell/Win64-OpenSSH/releases](https://github.com/PowerShell/Win32-OpenSSH/releases). We need a version for 64-bit Windows version: **OpenSSH-Win64.zip** (4 MB)

1. Extract the archive to the target directory: c:/tools/openssh64
2. Start PowerShell command prompt with the administrator privileges and go to the OpenSSH directory: cd c:/tools/openssh64
3. Generate SSH keys for the server (they are necessary to start sshd):  
   .\ssh-keygen.exe –A[](http://woshub.com/wp-content/uploads/2016/07/generating-openssh-keys.jpg)

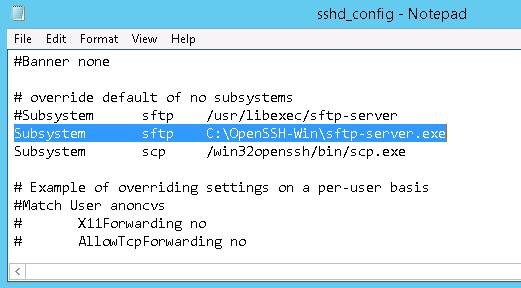
generating new host keys: RSA DSA ECDSA ED25519

1. Allow the incoming traffic on Port 22 (SSH server) in Windows Firewall:New-NetFirewallRule -Protocol TCP -LocalPort 22 -Direction Inbound -Action Allow -DisplayName SSH

[](http://woshub.com/wp-content/uploads/2016/07/New-NetFirewallRule-port-22.jpg)

**Note**. The previous command won’t work in a client OS. In this case another command is used:

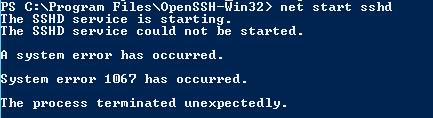
netsh advfirewall firewall add rule name='SSH Port' dir=in action=allow protocol=TCP localport=22

1. To enable authentication using keys:  
   powershell.exe .\install-sshlsa.ps1
2. Restart your server:  
   Restart-Computer
3. Open the configuration file C:\OpenSSH-Win\**sshd\_config** in any text editor, find and change the value of **Subsystem sftp** to **C:\OpenSSH-Win\sftp-server.exe** [](http://woshub.com/wp-content/uploads/2016/07/OpenSSH-Win-sftp-server.exe_.jpg)
4. Install sshd service  
   .\sshd.exe install
5. Specify that it has to be started automatically during the system boot and start it:Set-Service sshd -StartupType Automatic  
   Start-Service sshd

**Note**. In my case, SSHD in Windows Server 2012 R2 did not start returning the following error:

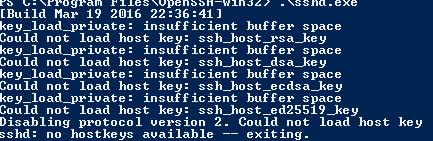
net start sshd

The SSHD service is starting.  
The SSHD service could not be started.  
A system error has occurred.  
System error 1067 has occurred.  
The process terminated unexpectedly.

[](http://woshub.com/wp-content/uploads/2016/07/System-error-1067-has-occurred.jpg)

When trying to start sshd.exe with no parameters manually, the error text was more informative, but still not enough for effective troubleshooting.

.\sshd.exe  
  
[Build Mar 19 2016 22:36:41]  
key\_load\_private: insufficient buffer space  
Could not load host key: ssh\_host\_rsa\_key  
key\_load\_private: insufficient buffer space  
Could not load host key: ssh\_host\_dsa\_key  
key\_load\_private: insufficient buffer space  
Could not load host key: ssh\_host\_ecdsa\_key  
key\_load\_private: insufficient buffer space  
Could not load host key: ssh\_host\_ed25519\_key  
Disabling protocol version 2. Could not load host key

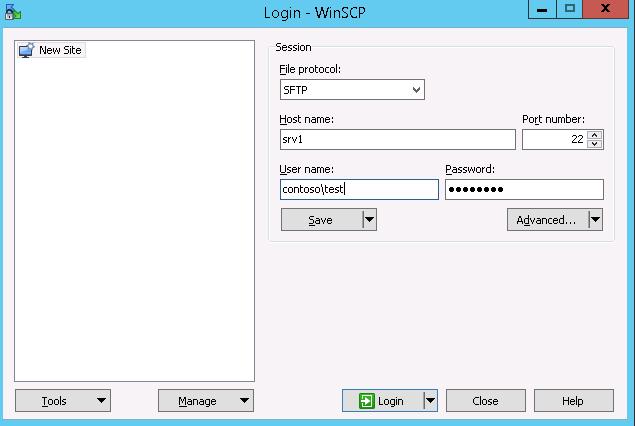
[](http://woshub.com/wp-content/uploads/2016/07/key_load_private-insufficient-buffer-space.jpg)

As it turned out, it is a well-known bug of the release as of March, 19, 2016. The developers promise to correct it in the next releases. Meanwhile, it is recommended to use **OpenSSH-Win64-1.1**.

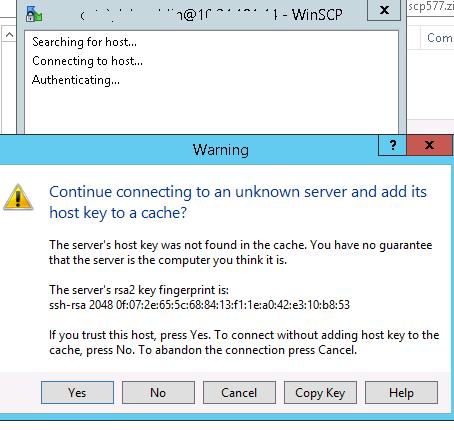
Test of the SFTP Connection

Let’s try to connect to the created SSH server by SFTP. To do it, use a free **WinSCP client.**

In the connection configuration window, select SFTP as the protocol of data transfer, specify the server name and the credentials of the Windows account, which is used for connection. (It is also possible to configure authentication using keys.)

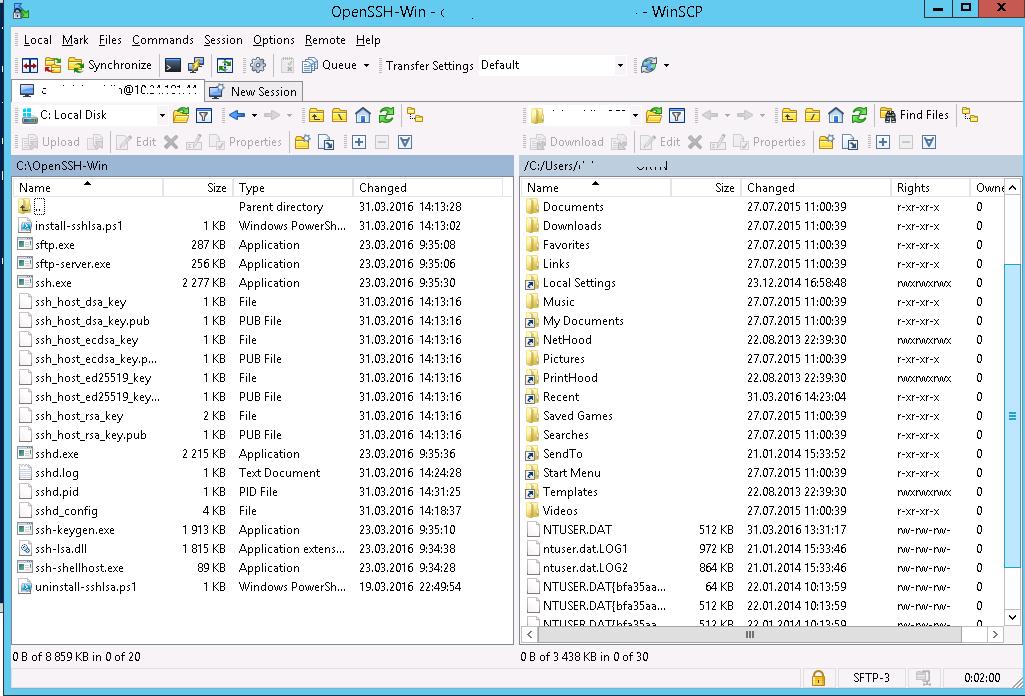
[](http://woshub.com/wp-content/uploads/2016/07/winscp-test-sftp-server.jpg)

When you try to connect for the first time, the following notification of the host key not found in the local cache appears.

[](http://woshub.com/wp-content/uploads/2016/07/rsa2-key-warning.jpg)

If you configured it right, a client would connect to the SFTP server and display the list of files in the user home directory (by default, it is the directory with the user profile).

Using the familiar interface of the file manager, you can copy files between the server and the client. Files are transferred using the protected SFTP.

[](http://woshub.com/wp-content/uploads/2016/07/connect-openssh-on-windows-using-winscp.jpg)

How to Uninstall Win64 OpenSSH

To uninstall Win64 OpenSSH from your system correctly:

1. Start PowerShell console with the administrator privileges
2. Stop the SSHD service:  
   Stop-Service sshd
3. Uninstall the service:.\sshd.exe uninstall
4. Uninstall the keys:  
   powershell .\uninstall-sshlsa.ps1