superuser

Command to copy client public key to Windows OpenSSH SFTP/SSH server authorized keys file

Asked 4 years, 11 months ago Modified 2 months ago Viewed 51k times

19

I have a Linux machine, and I need to sftp to a Windows SFTP server. So for first step, I create my own `id_rsa` file and the `id_rsa.pub` in my Linux machine.

Then I copy the text in the `id_rsa.pub` into the `id_rsa.pub` in the SFTP server.

And the `sftp` connection work correctly.

However, I would like to ask about the command to copy the public key from client to server. I have search in google and I get a command which is:

```
ssh-copy-id -i id_rsa.pub ftp_user*@10.7.8.32
```

But I hit the following error:

> 'exec' is not recognized as an internal or external command, operable program or batch file. The system cannot find the path specified.

```
[admin@wmdvvscibap01 ~]$ cd /home/admin/.ssh/
[admin@wmdvvscibap01 .ssh]$ ssh-copy-id -i id_rsa.pub ftp_cib_dev@10.8.1.79
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
Password Authentication:
ftp_cib_dev's password:
'exec' is not recognized as an internal or external command,
operable program or batch file.
The system cannot find the path specified.
[admin@wmdvvscibap01 .ssh]$
```

I believe there is some command exits for this right? Instead of I copy the public key manually to the SFTP server.

The SFTP version is SFTP protocol version 3.

linux windows ssh openssh sftp

Share Improve this question

Follow

edited Jun 25, 2019 at 6:46

Martin Prikryl

22.5k 10 83 164

asked Jun 21, 2019 at 6:33

Panadol Chong

291 1 2 6

6 Answers

Sorted by: Highest score (default)

10

`ssh-copy-id` script works only against *nix servers (or servers with *nix emulation), as it internally executes some *nix shell commands on the server (like `exec`, `sh`, `umask`, `rm`, `mkdir`, `tail`, `cat`, etc).

You can setup the key manually. I'm aware that you know that, but as there are subtle differences, when doing that on a Windows server, I'll mention it anyway for benefit of other readers.

Main steps are:

- Create the `.ssh` folder in your Windows account profile folder (typically in `C:\Users\username\.ssh`). Note that the location of the file for Administrators is overridden in the default `sshd_config` file to `%ALLUSERSPROFILE%\ssh\administrators_authorized_keys`.
- Create `authorized_keys` file in the folder and add your public key to it.
- Make sure that the ACL of the `.ssh` (or Administrator's `ssh`) folder and the `authorized_keys` are set so that only a respective Windows account have a write access to the folder and the file and the account that runs the server have a read access.

For details, see my guide for Setting up SSH public key authentication on Win32-OpenSSH.

If you want to do that from your local machine, you can do it using `sftp`. Particularly if you have no key on the server registered yet, you can just upload the `id_rsa.pub` file as `authorized_keys` file:

```
$ sftp martin@example.com
martin@example.com's password:
Connected to martin@example.com.
sftp> mkdir .ssh
sftp> cd .ssh
sftp> put id_rsa.pub authorized_keys
Uploading id_rsa.pub to /C:/Users/martin/.ssh/authorized_keys
id_rsa.pub                                    100%  401   197.5KB/s   00:00
sftp> bye
```

The above is basically, what `ssh-copy-id` does internally – Except that `ssh-copy-id` appends the `authorized_keys`, what plain `sftp` cannot do. If you need to append, you can download `authorized_keys` to the local machine, append it locally and re-upload it back.

Alternatively, you can setup the key from another Windows machine using *(my)* WinSCP client, with its *Install Public Key into Server* function.

See also my answer to Setting up public key authentication to Linux server from Windows (ppk private key).

Share Improve this answer Follow

edited Nov 30, 2023 at 7:06

answered Jun 21, 2019 at 7:14

Martin Prikryl
22.5k 10 83 164

3

You can follow Microsoft documentation to do it - https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh_keymanagement#deploying-the-public-key

Summary (for Administrator)

- Generate ssh key files using the command `ssh-key-gen` on your client.
- Copy `id_rsa.pub` file to windows server at location `C:\ProgramData\ssh\administrators_authorized_keys`.
- Update ACL on windows server using command

```
icacls.exe "C:\ProgramData\ssh\administrators_authorized_keys" /inheritance:r
/grant "Administrators:F" /grant "SYSTEM:F"
```

- Now you should be able to connect to your windows server from your client using ssh without password.

Share Improve this answer Follow

answered Jan 4, 2022 at 9:26

Suresh Kumar
131 1

2

The answer might **vary** based on whether the user **is an administrator**, and the **language** of the system.

Generate an ssh key

Use `ssh-keygen` to generate the public key `id_rsa.pub` and private key `id_rsa`.

```
ssh-keygen
```

Check if the user part of the Administrator group

List the groups with `whoami`.

```
whoami /groups
```

Check if you are part of the `BUILTIN\Administrators` **group**. The name might change based on your language. In French for example it's `BUILTIN\Administrateurs`.

Write the `authorized_keys` file

On Windows, there is an exception for **Administrators** and the file checked is `C:\ProgramData\ssh\administrators_authorized_keys`. Otherwise, the file check is `%USERPROFILE%\.ssh\authorized_keys`.

You can **remove** this **exception** by **commenting** the two last lines of **`sshd_config`** file.

```
# Match Group administrators
#     AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

Otherwise, as an **admin** just create the `C:\ProgramData\ssh\administrators_authorized_keys`, write in it the content of `id_rsa.pub`.

```
scp id_rsa.pub USERNAME@HOSTNAME:/ProgramData/ssh/administrators_authorized_keys
```

If you are a **user**, write the content of `id_rsa.pub` in the file `C:\Users\USER\.ssh\authorized_keys`.

Change permissions on the **`authorized_keys`**.

You can use `icacls.exe` to examine the rights of the file.

```
icacls.exe administrators_authorized_keys
```

OpenSSH will refuse to authenticate you if the rights are not correct on the `authorized_key` file.

Remove inheritance

```
icacls.exe administrators_authorized_keys /inheritance:r
```

Grant rights to System and Administrators group

```
icacls.exe administrators_authorized_keys /grant SYSTEM:F
icacls.exe administrators_authorized_keys /grant Administrators:F
```

You might need to change this last command to **match your language**. In French for example, the command will be.

```
icacls.exe administrators_authorized_keys /grant Administrateurs:F
```

Share Improve this answer Follow

edited Jan 22 at 10:12

answered Nov 29, 2023 at 21:49

Olivier Lasne
231 2 3

1 Created an account here just to say thank you! After 6 hours this fixed it. Jan 2024 , it was scp id_rsa.pub olivier@windows:/ProgramData/ssh/administrators_authorized_keys – Joseph Adam Jan 15 at 0:10

0

Use git-bash in Windows 10: cmd below

```
ssh-copy-id user@hostname.example.com
```

Share Improve this answer Follow

edited Nov 30, 2021 at 10:06
Toto
18k 67 32 44

answered Nov 30, 2021 at 9:44
Vikram S
101 1

That might work in *some* cases, but it won't take care of the specifics on the Win32-OpenSSH. – Martin Prikryl Nov 30, 2021 at 11:37

0

You can copy it with

```
type $env:USERPROFILE\.ssh\id_rsa.pub | ssh user@example.com "cat >>
.ssh/authorized_keys"
```

Share Improve this answer Follow

answered Jul 31, 2023 at 22:07
imaginabit
101 1

0

Kindly warning (copy of new ssh-key over an existing one):

If you are in the same situation like me and re-generate your ssh-key and for some reason `ssh-copy-id` -command does not work even with force, `sftp` has worked for me, when you set up ssh a second time (e.g. the password on your remote machine expires and you are forced to change it) the copy of the neew generated ssh key does not work properly.

```
sftp> put id_rsa.pub authorized_keys
```

If the file `authorized_keys` already exists, the ssh copy via sftp does not work until you delete `authorized_keys` and run the command above again.

So, if you have other hosts who are already connected to this remote machine and you delete the file only to overwrite it so you can connect, the other hosts could not connect via ssh anymore.

Share Improve this answer Follow

edited Mar 18 at 9:32

answered Mar 18 at 9:30

Michael_123
1 1