- Products
- Services
- Portfolio
- Blog
- About Us
- Contact Us
- Support

SFTP Tips & Tricks

Using Keyfiles To Access SFTP Services

You can use the private key .pem files to allow you to connect via SFTP on a server that only allows key access.

The trick is to get the .pem file that Amazon gives you onto the sever that you will be using to connect to the EC2 instance. When you store the .pem file on the local box, you will need to ensure the security level is set to 500 (r-x——).

Here is an example:

```
# sftp -o IdentityFile=my-amazon-given-key.pem root@domU-11-22-33-00-CC-11
```

We often use this trick to talk to our Amazon EC2 instances as they do not allow password based authentication by default. This is a good security mechanism as only people with an authorized key file can gain access. It also gives you a quick an easy way to shut down all access keys by disabling a single key file, essentially shutting down access from an entire group should there be a breach.

Create SFTP Logins Using Private Keyfiles

This is an example based on creating 3rd party access to SFTP on an Amazon EC2 instance. The article is written for system administrators that wish to grant SFTP access to their server using a private key file they distribute to their users. There can be multiple key files per username/directory.

1. Logon to the EC2 instance with a privileged (root?) account.
2. Create a keypair and save it to your PC.
3. Start puttygen on your PC.
    1. Conversion/Import – load the key file you saved in step 2.
    2. Save as a private key (I like to add the -priv.ppk extension).
    3. Copy the Key data from the top private key info box (Public key for pasting into OpenSSH authorized_keys file:).
4. Login to the server where you want the SFTP user to retrieve their files from.
5. Change to the home directory of the user you want to grant SFTP access to.
6. Create a .ssh directory.

    1. chmod 700 on that directory (rwx——)
    2. chmod 750 on that directory (rwxr-x—) to open access to other people in the same user group.
7. Create an authorized_keys file within the .ssh directory.
    1. Create a SINGLE LINE that has the fingerprint you copied from puttygen above.
    2. Save the file.
    3. Chmod 600 on that file (rw——-)
        1. Use mode 640 (rw-r——) to open access to other people in the same user group.

Now that you have the private key file from step 2.2 above, you can use that to login via PuTTY or SFTP from any system. The only thing you need is local access to that key file.

Using Private Keys with Filezilla and EC2

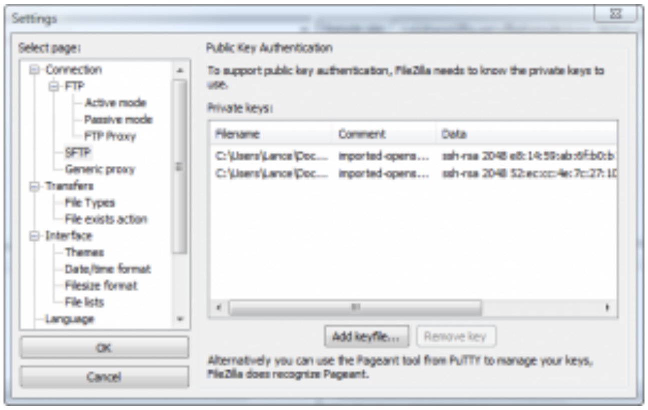
After completing the creation of the key file & server-side tweaks to accept that key, you can now use desktop clients such as Filezilla to access your FTP content.   This assumes the system administrator of the server you are connecting to has given you a key file and they have installed the handshake privelages in the authorized_keys file on the remote end.

Pageant Method

- Start by running pageant on your local system.
- Add key
- Find the key you generated with puttygen in step 3.2 above.
- Start filezilla
- In site manager enter the host name. This will be the same server you logged into on step 4 above.
- Servertype should be set to SFTP
- Logontype Normal
- User will be the name of the user that was given SFTP access (you created a .ssh/authorized_keys file in their home directory on the server)

Filezilla Specified Key Method

- Start Filezilla
- File/Site Manager – New Site
- Enter the host name. This will be the same server you logged into on step 4 from Create SFTP Logins Using Private Keyfiles
- Servertype should be set to SFTP
- Logontype Normal
- User will be the name of the user that was given SFTP access (you created a .ssh/authorized_keys file in their home directory on the server)
- Click OK (NOT CONNECT)
- Edit/Settings
    - Connection/SFTP
    - Add keyfile… and select the private keyfile you generated with puttygen above.



Public Key Authentication

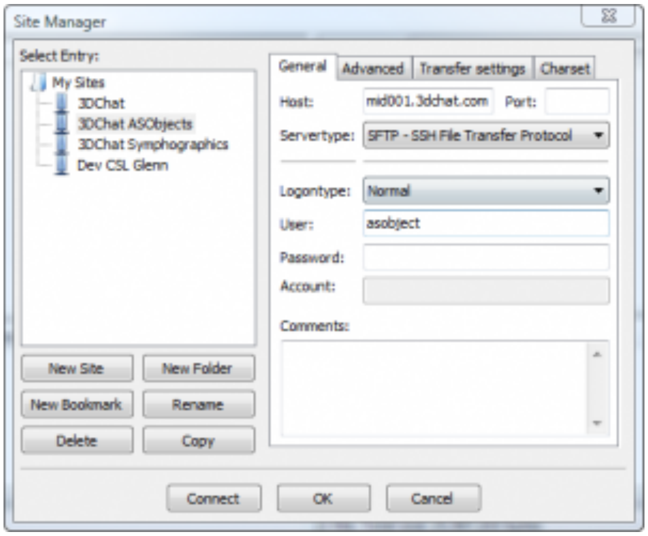
To support public key authentication, FileZilla needs to know the private keys to use.

Private keys:

Filename	Comment	Data
C:\Users\Lance\Doc...	imported-opens...	ssh-rsa 2048 e8:14:59:ab:6f:b0:b
C:\Users\Lance\Doc...	imported-opens...	ssh-rsa 2048 52:ec:cc:4e:7c:27:1C

Alternatively you can use the Pageant tool from PuTTY to manage your keys, FileZilla does recognize Pageant.

Filezilla - Edit Settings



Host: mid001.3dchat.com Port:

Servertype: SFTP - SSH File Transfer Protocol

Logontype: Normal

User: asobject

Password:

Account:

Comments:

Filezilla Site Manager

Now connect to that site. Filezilla will read through the keys and find the right key for the user/server pair that you are connecting to.

Related posts:

1. Logon To Your Linux Box Using SSH Keys
2. Creating and Installing SSL Certs via SSH
3. Upgrading Logwatch on CentOS 5
4. Holy Hell, Properties!
5. Working With Git

0 Comment | Posted in Networking Utilities,SSH,Security,Tips & Tricks,blog by lcleveland on December 09, 2009

Leave a comment

Name (required)

Mail (required)

Website

Comment (required)

○

Search Articles

Search for: Search

Article Categories

Select Category

Tags

.net apache at&t Bash blog Charleston SC cut Database default now directory droid Emacs escaping find full text search Gadgets git innodb installer Javascript js Linux lisp login logwatch MB MiB microsoft myisam mysql networking nsis on delete Perl php postgresql programming sed server sftp sql syntax SSH terminology windows Wordpress

Recent Articles

- Changing Network Device Priorities In Vista
- WordPress – Sharing A Base Class Amongst Plugins
- Using Find To Help Manage Files On Linux
- Cleaner Git Log With Merges
- What’s Wrong With Guru.com
- More PHP Woes
- Using Common Sense With Perl
- More Info From Git Branches
- Windows XP – Resolving Aquiring Network Address Problems
- Perl Regular Expression \K Trick

- HTTP Errors When Uploading/Connecting in WordPress
- Droid Incredible Crashes Wifi Networks
- array_key_exists() versus isset()
- Upgrading Logwatch on CentOS 5
- iPhone versus Droid Incredible

359 Wando Place Drive, Ste D, Mt Pleasant SC 29464
Phone: (888) 508-4510, Fax: (843) 225-1337, Email: info@cybersprocket.com