Connect to an AWS EC2 Instance – Windows & PuTTY

When you have created and launched an AWS Linux EC2 instance, you can connect to it from your computer using the SSH protocol. PuTTY is a free SSH client that allows you to do this from a local computer running Windows. Once the connection has been established, you work within the EC2 instance just like you would on a local computer running Linux.

Overview of the steps in this recipe:

A. Prerequisites
B. Generate a PuTTY private key file
C. Connect to EC2 instance

A) Prerequisites

a. You must have an AWS account. If you don't have an account, click HERE to create one.

> ***Note:*** You will need to provide credit card information for your new account.

b. You will need to create and launch a Linux EC2 instance to connect to. Instructions for this are found in the recipe titled "Create a Basic Elastic Cloud Compute (EC2) Instance."

B) Generate a PuTTY Private Key (.ppk) file

1. Download and install PuTTY.
   https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. Open the folder that PuTTY was installed to (default path is **C: > Program Files > PuTTY**).
3. Double click on the file **puttygen.exe**.

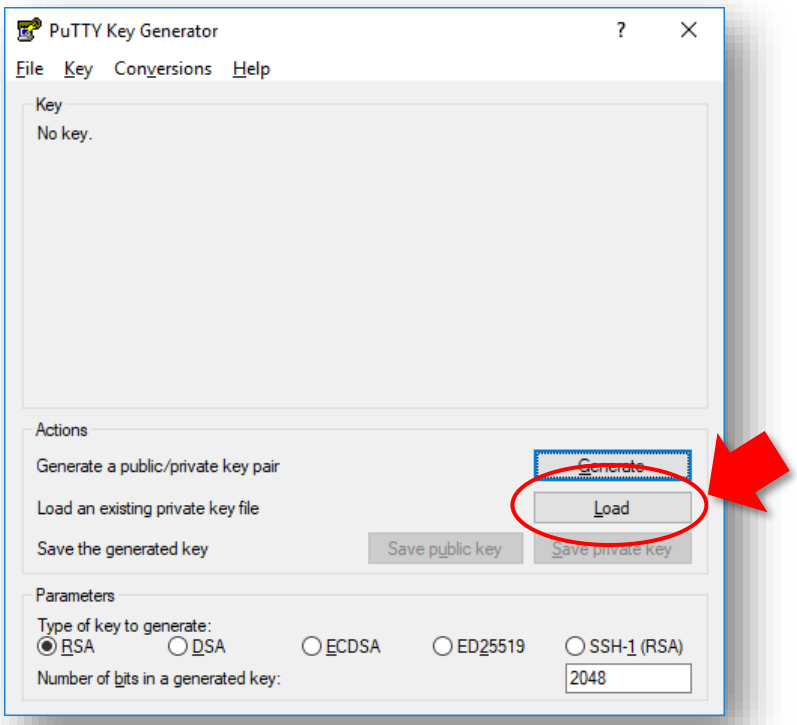


Figure 1

4. In PuTTY Key Generator (Fig. 1), click the **Load** button and navigate to the folder that contains the private key file *(.pem)* created during the EC2 configuration process.
5. Click on the **PuTTY Private Key Files** button in the lower right corner of the window (Fig. 2) and select *All Files (*.*)*.

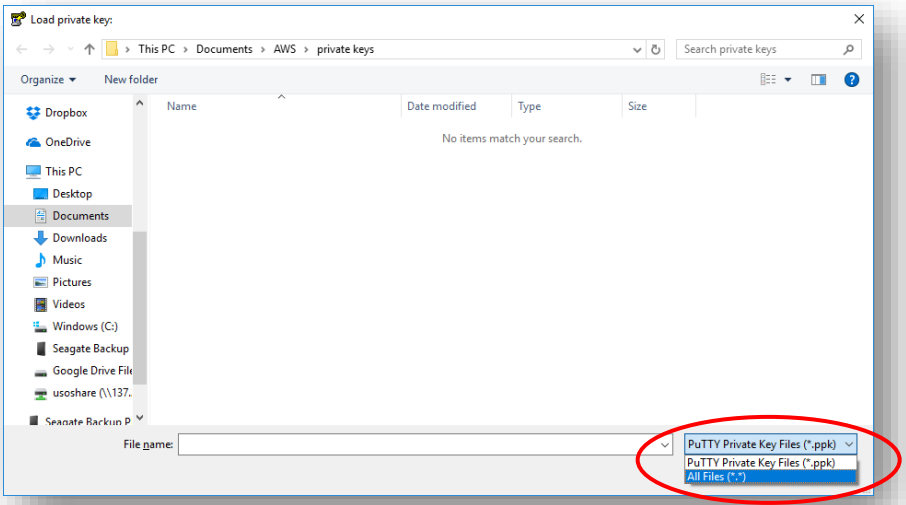


Figure 2

6. Select your private key file *(.pem)* and click **Open** (Fig. 3).

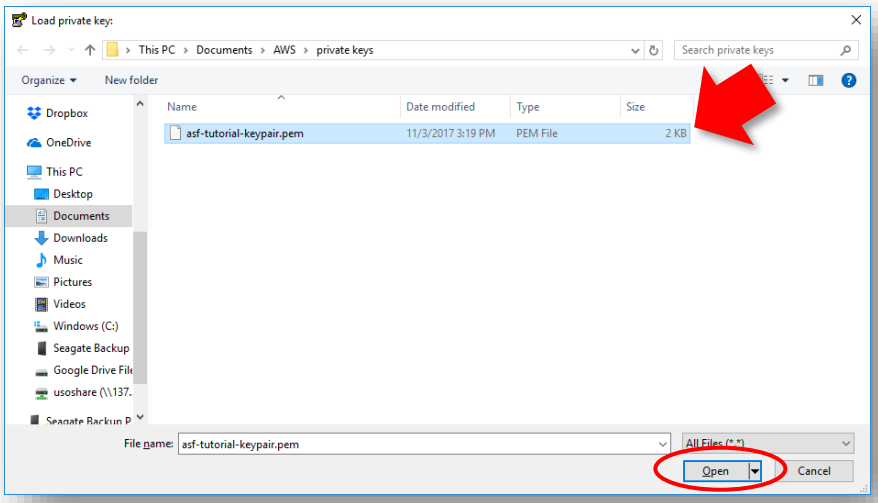
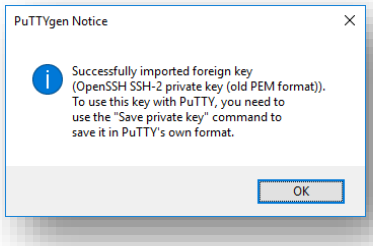
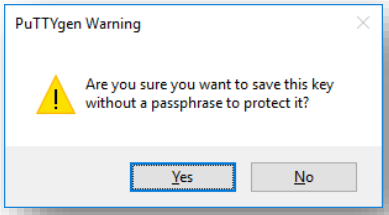


Figure 3

7. Click **OK** to close the *PuTTYgen Notice* pop-up window.
8. In *PuTTY Key Generator*, make sure *Type of key to generate* value is set to **RSA** (Fig. 4).
9. Click **Save private key** and then **Yes** to close the *PuTTYgen Warning* pop-up window.





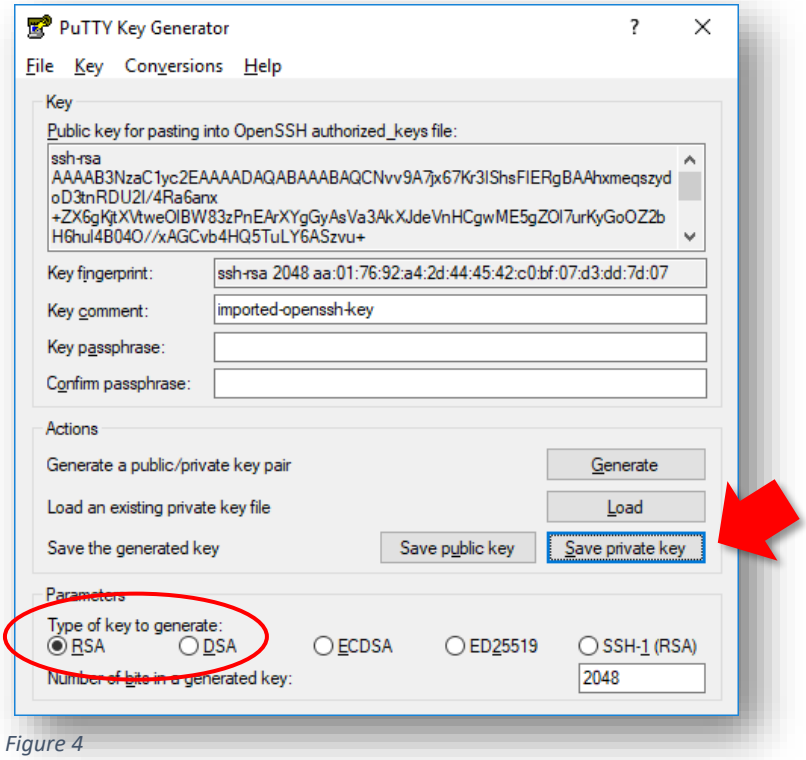


Figure 4

10. Navigate to the location you want to store your *PuTTY Private Key file (.ppk)* and give it a name (Fig. 5)..

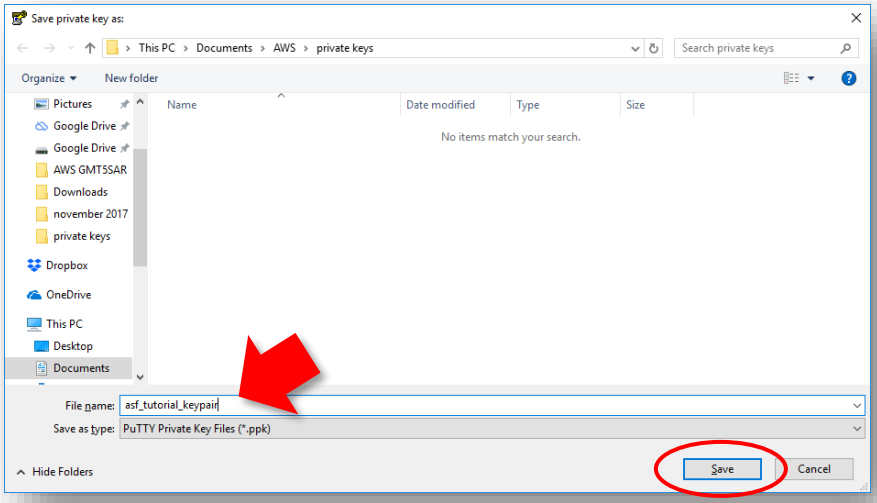


Figure 5

11. Click **Save**.
12. Close the *PuTTY Key Generator* window.

C) Connect to EC2

13. Open PuTTY by clicking on the desktop icon or the **putty.exe** file in the PuTTY folder.
14. In the *Host Name (or IP address)* box, type **ubuntu@your_public_DNS** (Fig. 6) (**1**).
    a. *Note*: The **Public DNS** for your instance is displayed in AWS in the EC2 Management Console *Instance Description* in the middle of the screen.
15. Make sure:
    a. *Port* is set to **22** (**2**)
    b. *Connection type* is **SSH** (**3**)

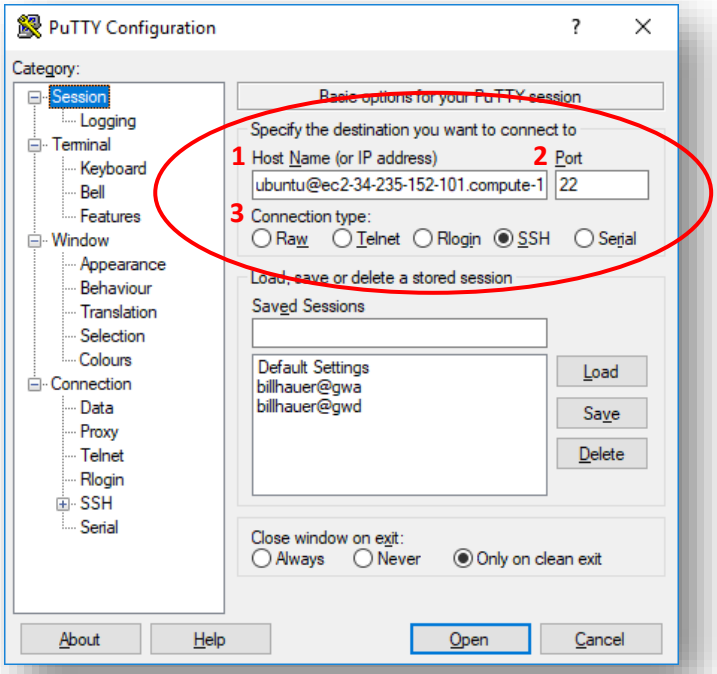


Figure 6

16. In the *Category* pane on the left of the PuTTY Configuration window, under *Connection* click on the **+** next to *SSH* to expand the choices (Fig. 7) (**4**), then click on *Auth* ((Fig. 7) (**5**).
17. Under *Authentication parameters*, click **Browse** and navigate to the directory where your *PuTTY Private Key (.ppk)* file is located (**6**).
    a. Click on the (.ppk) file to select it
18. Click **Open**.

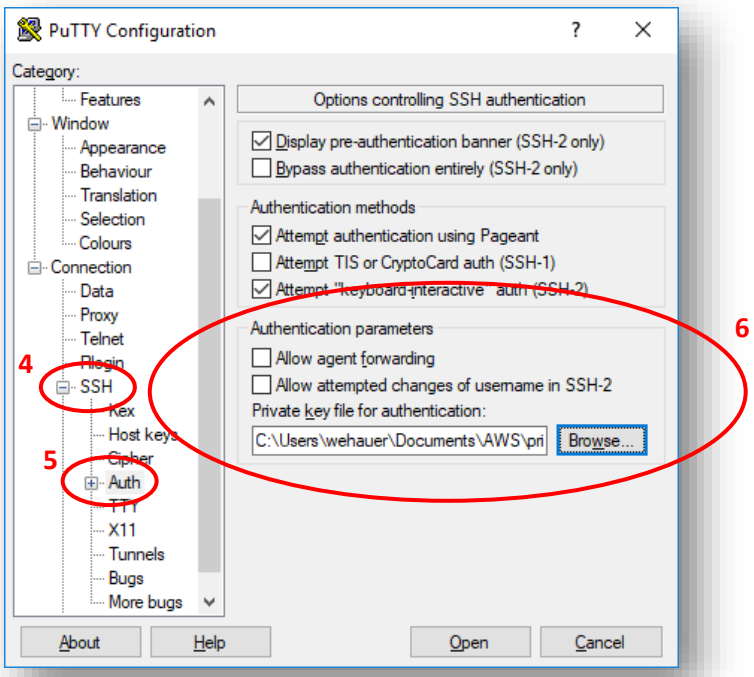


Figure 7

Note: If you want to save these settings to use later, navigate to **Sessions** in the PuTTY **Category** tree. Enter a name in the **Saved Sessions** box and click **Save** on the right.

19. Click **Open** in *PuTTY Configuration* to connect to your Instance.
    a. If this is the first time you have connected to your Instance, a "PuTTY Security Alert" will ask you whether to proceed with the connection (Fig. 8).
    b. Click **Yes** to complete the connection.
    c. The EC2 instance window will appear (black screen below).

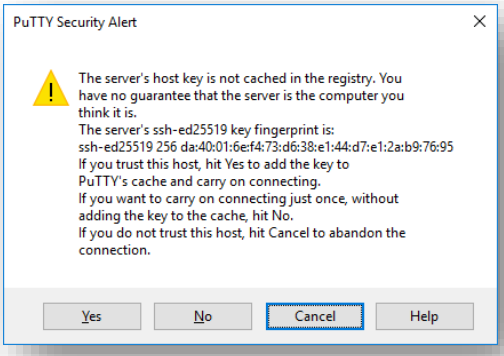


Figure 9

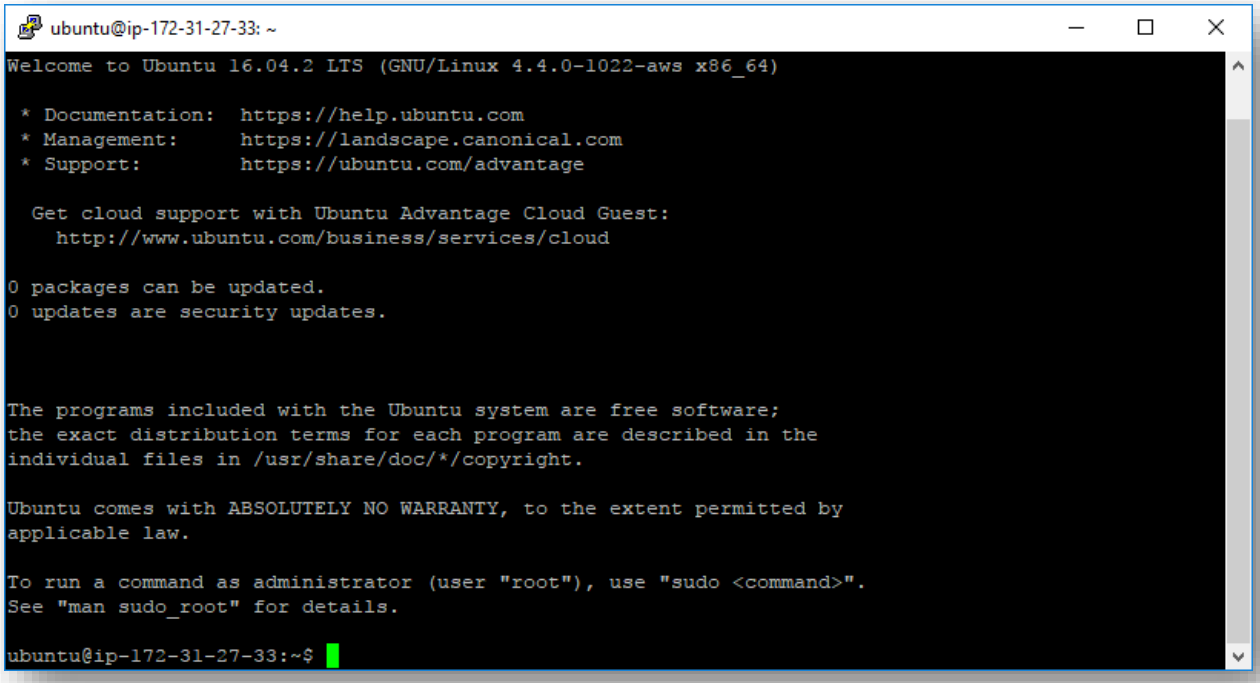


Figure 8. ***You are now connected to your EC2 instance!***