COS20019 - Software Development for Cloud Computing

How to remote access & manage files on your Linux EC2 instance

1. Create your own key pair to access AWS (one off)

Key Pair is used for securely accessing your EC2 instances. A key pair consists of two parts: public key and private key. The public key is embedded in your EC2 instance, while you use the private key to sign in securely. You can create multiple EC2 instances using the same key pair or assign different key pairs to individual EC2 instances. In this unit, you only need to create one key pair. You can get to the key pair management page via the "Network&Security - Key Pairs" in the menu on the left hand side of the EC2 dashboard in order to create or delete the key pairs.

Note: You need to store the private key file (in .pem format) safely, say on your USB or on your cloud folder, since it is generated only once when you created it. You will not be able to download it again in case you lost it, leading to you loosing access to your EC2 instances created with the lost key.

The following steps are for Windows users. Mac OS and Linux user see the note below:

2. Convert .PEM file to .PPK file

You need a private key in .ppk format in order to SSH into your Linux instance. Follow the steps below to convert the private key in .pem format to .ppk format:

- Download PuTTy and PuTTygen from here.
- Start PuTTygen to convert .pem file to .ppk file.
- Select 'Load an existing private key file' and select your .pem file.
- PuTTygen will convert this file to a .ppk file. Now click 'Save private key' to save the generated .ppk file. A passphase is not required here (unless you need additional security).

3. Connect to your Linux EC2 instance with PuTTy

Given the .ppk private key above, you can SSH into your Linux EC2 instance by:

- Launch PuTTY and enter your EC2's public DNS as the host name.
- Navigate to Connection – SSH – Auth then click 'Browse' to select your .ppk private key file exported from PuTTygen above.
- Click 'Open'. When connection comes up, enter the user name of your EC2 instance. For the Amazon Linux AMI or Amazon Linux 2, the default user name is `ec2-user`.

Now you will be able to control your Linux EC2 instance via the terminal.

4. Exchange files to your Linux EC2 instance with WinSCP

A quick and easy way to transfer/manage files on your Linux EC2 instance is to use WinSCP, a Secure Copy and Paste file transfer client:

- Download WinSCP from here.
- Launch WinSCP. In the promted Login dialog box, enter your EC2's public DNS as the host name and `ec2-user` as the user name. File protocol is SFTP.
- Click 'Advanced…' then navigate to SSH – Authentication.
- Select your private key file (.ppk) then hit 'OK'.
- Click 'Login'. Now you can start transfer files with your Linux EC2 instance.

Note for Mac OS and Linux user

Mac OS and Linux use .pem format private keys.

To connect to your EC2 instance, run the following commands in Terminal (but substituting values as explained below):

```
chmod 400 <path and name of pem file>

ssh -i <path and name of pem> ec2-user@<Public IP>
```

- For **<path and name of pem file>**, substitute the path/filename to the .pem file you downloaded.
- For **<Public IP>**, enter the public IP address of your EC2 instance, which is shown to the left of the instructions you are currently reading.

To transfer files to the EC2 instance can use the terminal command line or your Mac / Linux compatible file utility of choice (e.g. FileZilla, Cyberduck).