Azure Workshop Preparation

It's simple to create a MarkLogic cluster in Microsoft Azure. But before you do, you should become familiar with the process. It's highly recommended to read through the MarkLogic Server on Microsoft® Azure® Guide.

Also, make sure you have done the following:

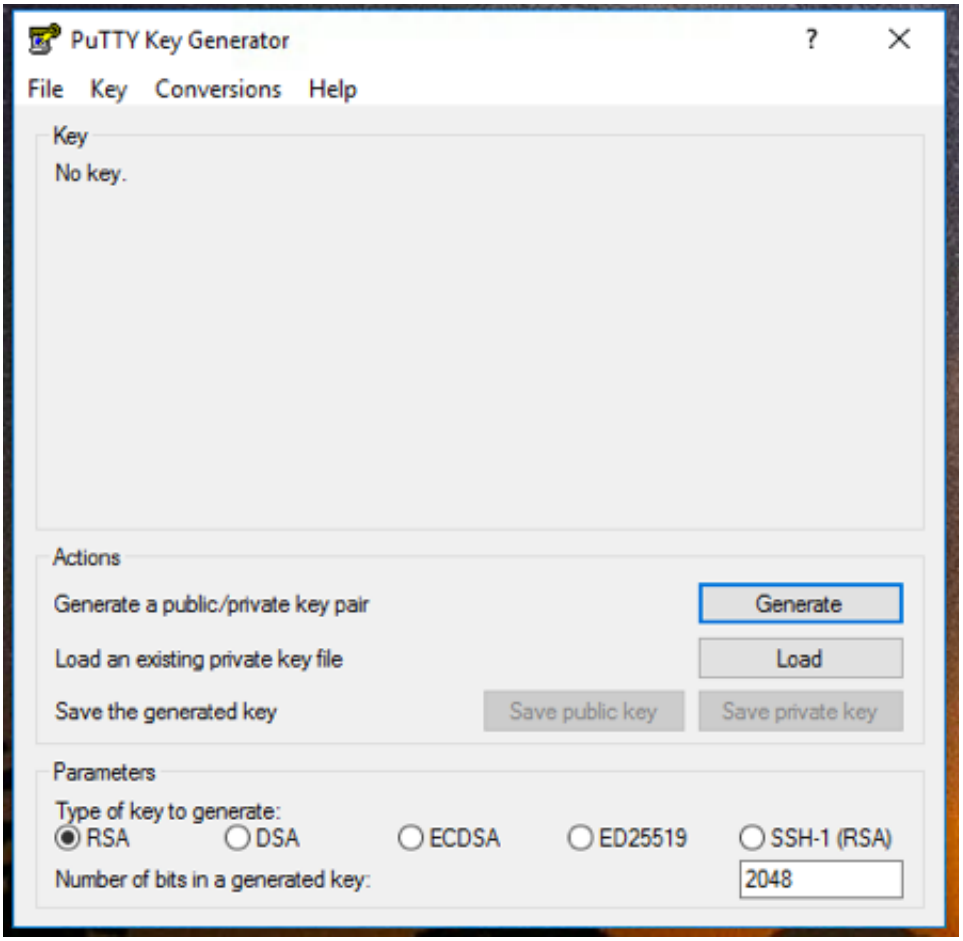
- If you don't already have a Microsoft account, create one.
  Creating you Azure free account today
- Access the *Azure portal*.
  Create and share dashboards in the Azure portal.
- Create an account subscription that running resources can be billed to.
- Ensure you have Putty if you are using Windows. MacOS and other *nix users already have SSH in their terminal.
- An SSH key is required for this workshop. A placeholder one will be supplied, but outside of the workshop you would need to have your own generated. See the following sections for more details.

Creating a public SSH key (OPTIONAL)

Creating a public SSH key (on Windows)

To create the public SSH key on Windows, we are going to assume that you have already installed the Putty suite which includes the *PuTTYgen* utility.

1. Launch the *PuTTYgen* utility.

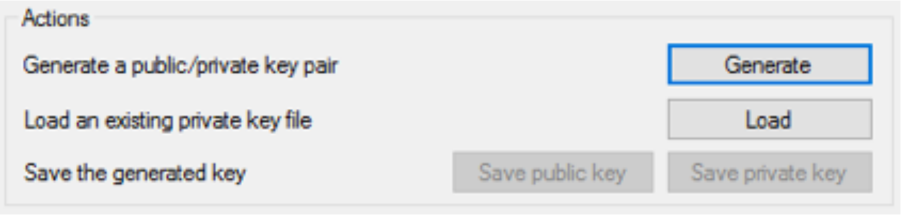


No key.

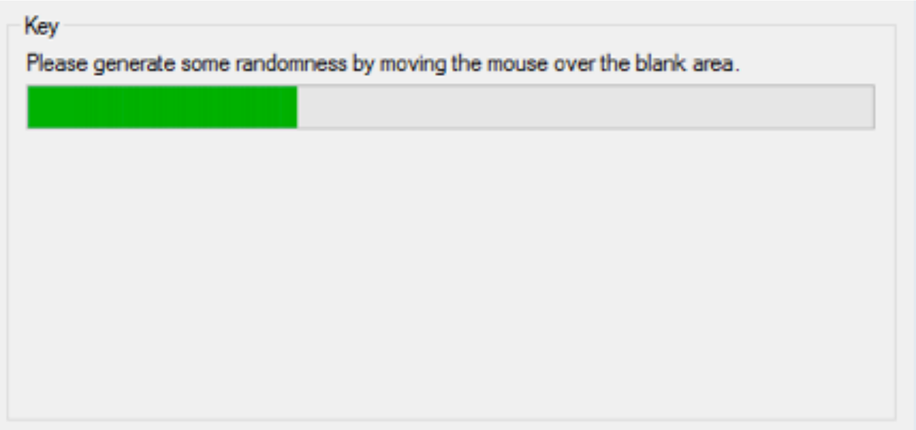
Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

2. Click the **Generate** button.

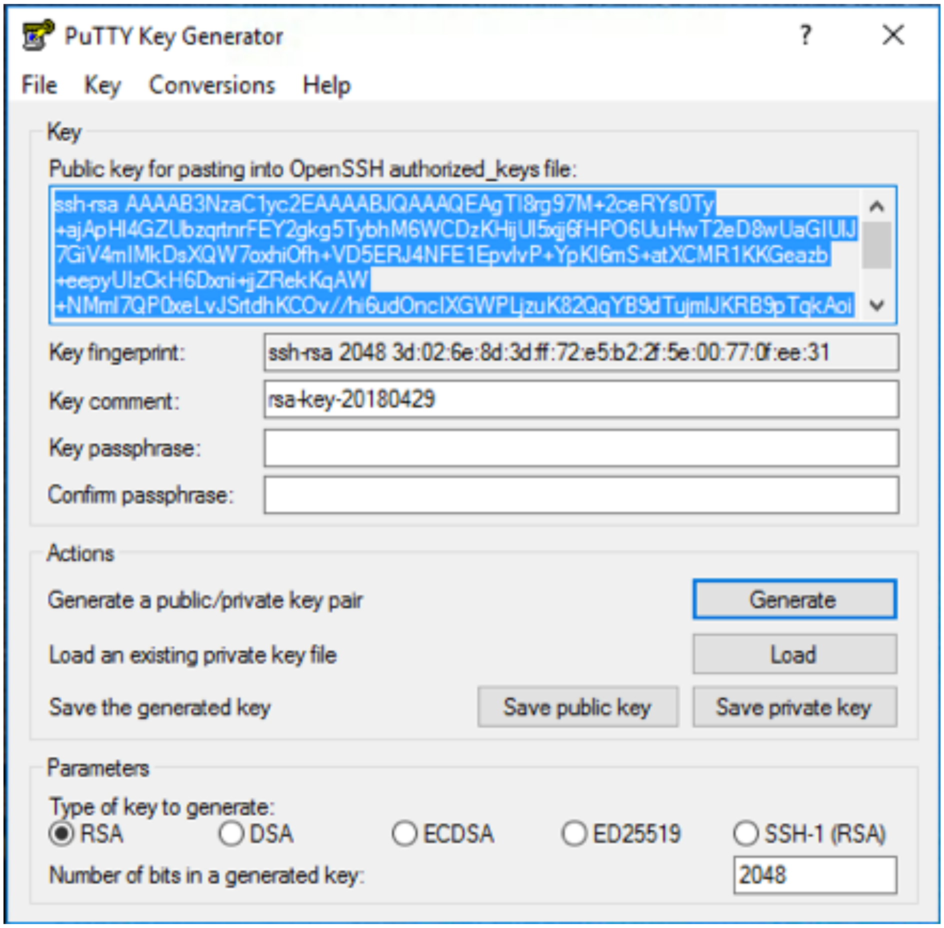


3. Wiggle the mouse around inside the blank space in the application window to create some randomness.



Please generate some randomness by moving the mouse over the blank area.

4. Once the application has collected enough input, the key pair will be generated.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAgTI8rg97M+2ceRYs0Ty
+ajApHI4GZUbzqrtnrFEY2gkg5TybhM6WCDzKHijUI5xjj6fHPO6UuHwT2eD8wUaGIUIJ
7GiV4mIMkDsXQW7oxhiOfh+VD5ERJ4NFE1EpvlvP+YpKI6mS+atXCMR1KKGeazb
+eepyUIzCkH6Dxni+jjZRekKqAW
+NMmI7QP0xeLvJSrtdhKCOv//hi6udOncIXGWPLjzuK82QqYB9dTujmIJKRB9pTqkAoi
```

Key fingerprint: ssh-rsa 2048 3d:02:6e:8d:3d:ff:72:e5:b2:2f:5e:00:77:0f:ee:31

Key comment: rsa-key-20180429

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

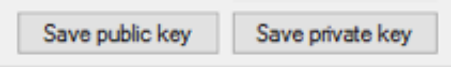
Save the generated key

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

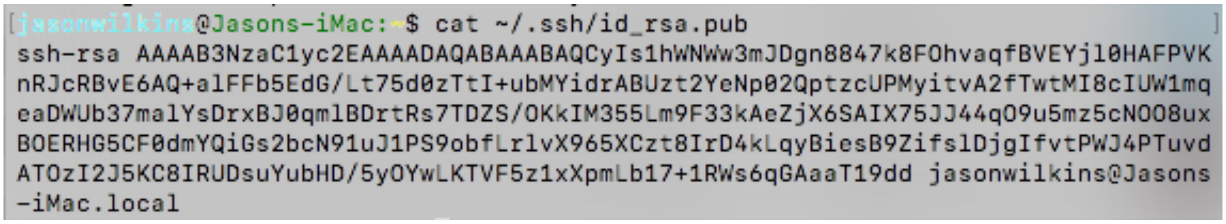
5. Click on the **Save public key** and the **Save private key** buttons in turn to save both the public and private keys that were generated. Please remember where these are stored as the public key will be needed for Unit 1.



Checking for an SSH key (on MacOS)

1. Open a command *Terminal*.
2. Try to list the contents of your public SSH key, if it exists.

`cat ~/.ssh/id_rsa.pub`



```
[jasonwilkins@Jasons-iMac:~$ cat ~/.ssh/id_rsa.pub                                                        ]
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCyIs1hWNWw3mJDgn8847k8FOhvaqfBVEYjl0HAFPVK
nRJcRBvE6AQ+alFFb5EdG/Lt75d0zTtI+ubMYidrABUzt2YeNp02QptzcUPMyitvA2fTwtMI8cIUW1mq
eaDWUb37malYsDrxBJ0qmlBDrtRs7TDZS/OKkIM355Lm9F33kAeZjX6SAIX75JJ44qO9u5mz5cNOO8ux
BOERHG5CF0dmYQiGs2bcN91uJ1PS9obfLrlvX965XCzt8IrD4kLqyBiesB9ZifslDjgIfvtPWJ4PTuvd
ATOzI2J5KC8IRUDsuYubHD/5yOYwLKTVF5z1xXpmLb17+1RWs6qGAaaT19dd jasonwilkins@Jasons
-iMac.local
```

> If the return is `No such file or directory`, then you need to generate a public key. Otherwise, make a note of it as we will need it in Unit 1.

Creating a public SSH key (on MacOS and most *nix)

1. Open a command *Terminal*.
2. Issue the following command:
   `ssh-keygen -t rsa`
3. Press **Enter** to accept the default location, but make note of where it is for your OS.
4. If desired type in a passphrase and press the **Enter** key. You can also just press the **Enter** key to accept the default (no passphrase). While easier to remember, from a security perspective it is not advised to leave this blank.
5. Confirm the passphrase as entered in the previous step.

> At this point the SSH key should be generated and available. Follow the instructions in the previous section, Checking for an SSH key (on MacOS), and use the directory that was listed in step 3.