# Lab Answer Key: Module 4: Virtual Machines

## Lab 1: Creating a Linux Virtual Machine

Please note that the virtual machine that you will create in this lab will also be used in the next lab of this course.

Lab exercises:

1. Create cryptographic keys
2. Create and connect to a Linux virtual machine

### Exercise 1: Create cryptographic keys

* [Windows Instructions](#windows-instructions)
* [Linux/Mac Instructions](#linux-mac-instructions)

Scenario: In this exercise you will create cryptographic keys that you will use to connect via PuTTY to the Azure virtual machine that you deploy later in this lab.

#### Windows Instructions

The main tasks for this exercise are as follows:

1. Install Git for Windows
2. Create a key pair
3. Create a private key for PuTTY

Task 1: Install Git for Windows

1. Using a web browser, navigate to https://git-for-windows.github.io/
2. Click on the **Download** link.
3. When prompted whether to run or save the Git executable, click **Run**.
4. In the Git 2.11.0 Setup wizard, accept the default settings to complete the install.
5. Once the install completes, on the **Completing the Git Setup Wizard** page, select the **Launch Git Bash** checkbox and click **Finish**. Alternatively, from the Start menu (or screen), start **Git Bash**.

Task 2: Create a key pair

1. In the **Git Bash window**, run the following:

* openssl.exe req -x509 -nodes -days 365 -newkey rsa:2048 \  
   -keyout myPrivateKey.key -out myCert.pem

1. When prompted, provide the information to be incorporated into the certificate you are generating, including country code, state or province, locality name, organization name, organizational unit, common name, and email address (for the purpose of this lab, you can use made up values).
2. Generate a public key by running:

* openssl.exe rsa -pubout -in myPrivateKey.key -out myPublicKey.key

Task 3: Create a private key for PuTTY

1. Convert the private key you generated in the previous task into a private key that you will be able to use with the PuTTY utility. In the **Git Bash** window, run the following:

* openssl rsa -in ./myPrivateKey.key -out myPrivateKey\_rsa

1. Using a web browser navigate to the [PuTTY Website](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).
2. Download puttygen.exe to the C:\Users\<username> folder, where <username> is your Windows user account name. This is the same location where the keys you generated in the previous task reside.
3. In the File Explorer window, double-click puttygen.exe.
4. In the **PuTTY Key Generator** window, click **Load**.
5. In the **Load private key** dialog box, make sure that the current directory is C:\Users\<username>, where <username> is the name of your user account, change filter to **All Files (*.*)**, select **myPrivateKey\_rsa** and click **Open**.
6. In the **PuTTYgen Notice** dialog box, click **OK**.
7. Copy the entire content of the **Public key for pasting into OpenSSH authorized\_keys file** section of the **PuTTY Key Generator** window into Clipboard.
8. In the **PuTTY Key Generator** window, click **Save private key**
9. Save the private key as myPrivateKey\_rsa.ppk in the C:\Users\<username> directory (where <username>is your Windows user name). Click **Yes** in the **PuTTYgen Warning** dialog box, when prompted whether to save the key without a passphrase to protect it. Note that you have the option of protecting it with a passphrase. >*Note: Outside of a lab environment, you should use a passphrase and file >system permission to protect your private key.*

#### Mac/Linux Instructions

Task 1: Verify openSSL is installed

This is an incomplete list. Some commands may require sudo.  
  
If the output of `which openssl; echo $?` is `1`, then openssl is not  
installed.  
  
\* Mac: `brew install openssl`  
\* Ubuntu: `apt install openssl`  
\* RedHat: `yum install openssl`  
\* Arch: `pacman -S openssl`

Task 2: Create your key

ssh-keygen -t rsa -f ~/myLabKey

*Please note that we're creating a pair of files in your user home directory. myLabKey is the private key, and myLabKey.pub is the public key. These files are typically stored in ~/.ssh*

### Exercise 2: Create and connect to a Linux virtual machine

Scenario: In this exercise you will create a new Linux virtual machine by using the [Azure Portal](https://portal.azure.com) and use the key you generated to connect to it.

The main tasks for this exercise are as follows:

1. Create a new Linux virtual machine by using the [Azure Portal](https://portal.azure.com)
2. Connect to the Linux virtual machine

#### Task 1: Create a new virtual machine

1. Using a web browser, navigate to the [Azure Portal](https://portal.azure.com)
2. Click on the **+Create a resource** link.
3. Select Compute in the blade that comes up.
4. In the Compute blade select **See all**.
5. In the Filter text box, type **Ubuntu Server** and press **Enter**
6. In the list of results, click the latest recommended Ubuntu Server ("Ubuntu Server xx.xx LTS").
7. Check to ensure the deployment type is set to **Resource Manager**
8. Click **Create**.
9. On the Basics blade, specify the following and click **OK**.
   * Name: **LabLinuxVM**
   * VM disk type: **HDD**
   * User name: **student**
   * Authentication type: **SSH public key**
   * SSH public key: paste the content of the public key file (Windows: myPublicKey.key, Mac/Linux: myLabKey.pub)
   * Resource group: create a new resource group called **LabLinuxRG**
   * Location: an Azure region closest to your physical location
10. On the Choose a size blade:
    * Click **"View all"**
    * Use your browser's find function to locate the **DS1\_V2** size and click it to make it the selection.
    * Click the **Select** button on the bottom of the blade.
11. On the **Settings** blade, accept the default settings and click **OK**.
12. On the **Summary** blade, click **OK**

#### Task 2: Connect to the Linux virtual machine

**Note**: You need to wait until the new virtual machine has been provisioned. This should take a couple of minutes. The [Azure Portal](https://portal.azure.com) will automatically display the new blade showing the settings of the new virtual machine.

Before you begin:

1. Navigate to the LabLinuxVM blade in the [Azure Portal](https://portal.azure.com).
2. Click on the **Overview** section.
3. Note the *Public IP address* assigned to the VM

Skip to:

* [Windows Instructions](#using-putty)
* [Linux/Mac Instructions](#using-openssh)

Using Putty

1. Using a web browser, navigate to the [PuTTY Website](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html)
2. Download putty.exe to your computer and click **Run** when prompted.
3. In the **PuTTY Configuration** window, enter the public IP address of your linux VM.
4. In the **Category** section of the **PuTTY Configuration** window, expand the **Connection->SSH** nodes and click **Auth**.
5. Click **Browse** next to the **Private key file for authentication** text box.
6. In the **Select private key file** dialog box, navigate to the C:\Users\<username> directory (where <username> is your Windows user name), select myPrivateKey\_rsa.ppk and click **Open**.
7. When prompted by the **PuTTY Security Alert**, click **Yes**.
8. In the **PuTTY** window, when prompted for the username, type in **student** and verify that you have successfully authenticated.

Using openSSH

1. Change the permissions on your private key.

* bash chmod 600 ~/myLabKey

1. Login to the virtual machine. Replace <ip-address> with the public IP address of your VM.

* ssh -i ~/myPublicKey student@<ip-address>