NeCTAR Use Tutorial

By Rahul Sharma

Introduction

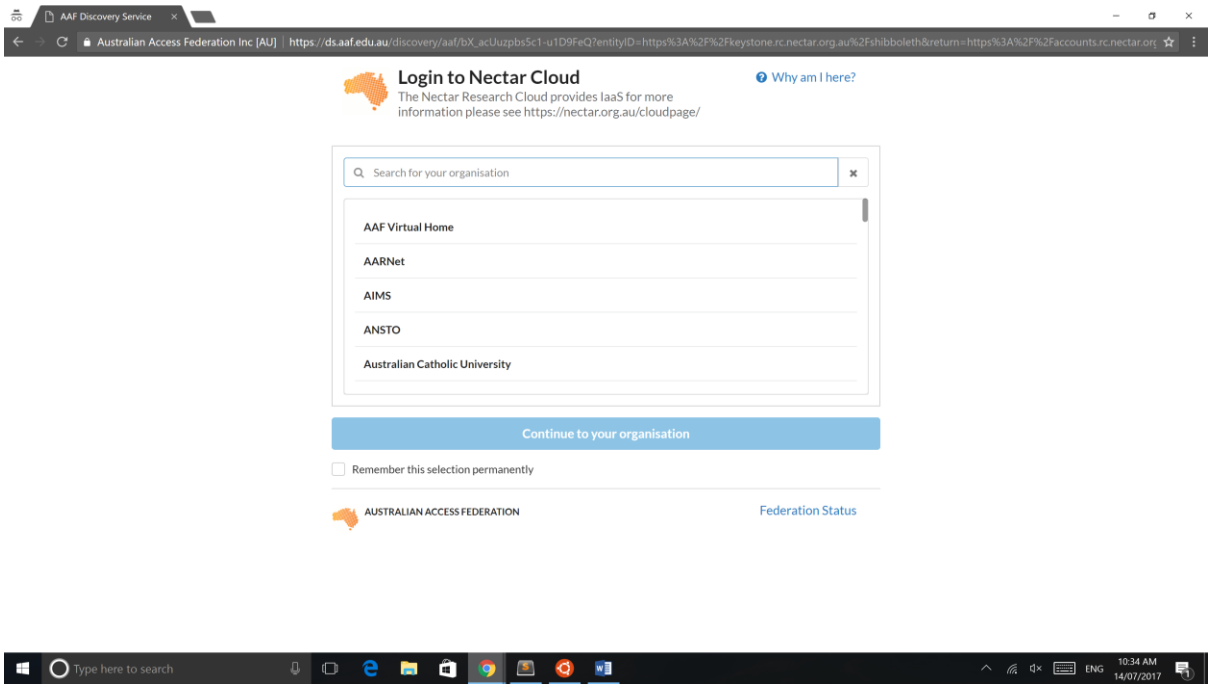
This guide will assist students in learning how to use the compute service offered by NeCTAR (Reseach cloud deployed using OpenStack). This guide is not meant to be comprehensive in regards to the various services available in NeCTAR but will act as an initial guide for you to explore NeCTAR yourself. **Note: A list of Warnings are present at the end of this document, please review them before use.**

Access the NeCTAR Platform

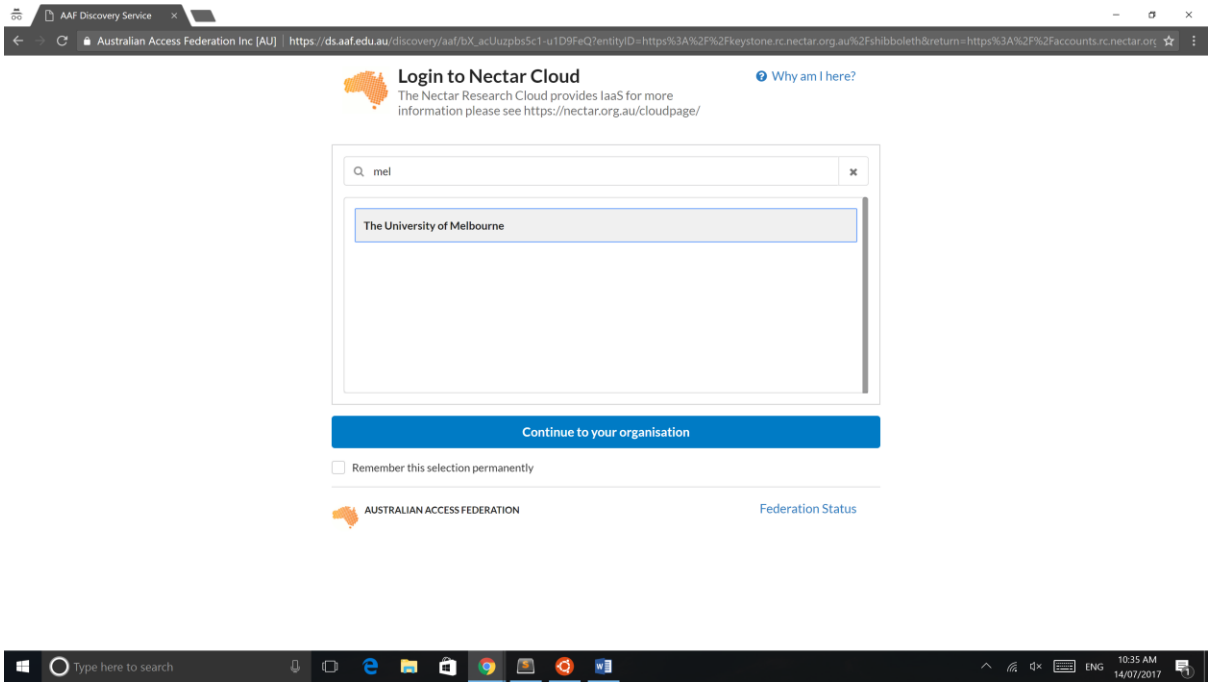
To gain access to NeCTAR's dashboard, click on the following link:

https://dashboard.rc.nectar.org.au/auth/login/?next=/

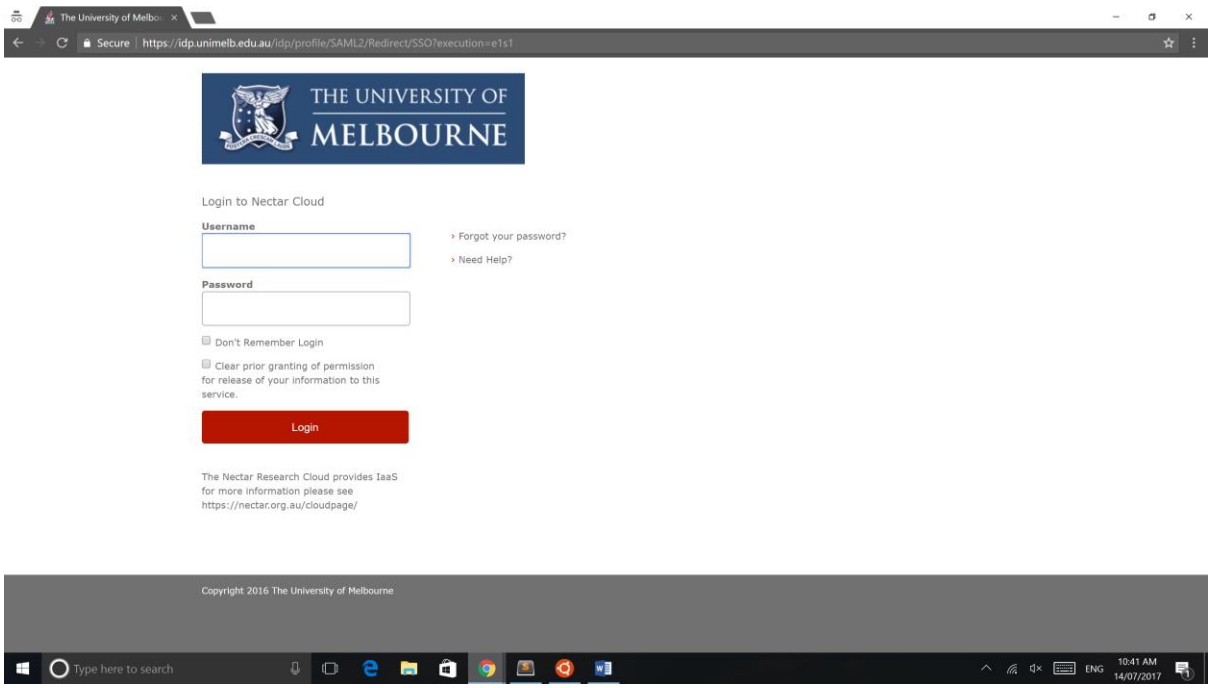
This link will lead you to a federated access webpage (uses Shibboleth). Click on "Log In". You will now see the following web page:



In the search bar type: Melbourne or University of Melbourne (Longer Route) and you will find the entry for the University of Melbourne. Choose that and click on "Continue to your organization".

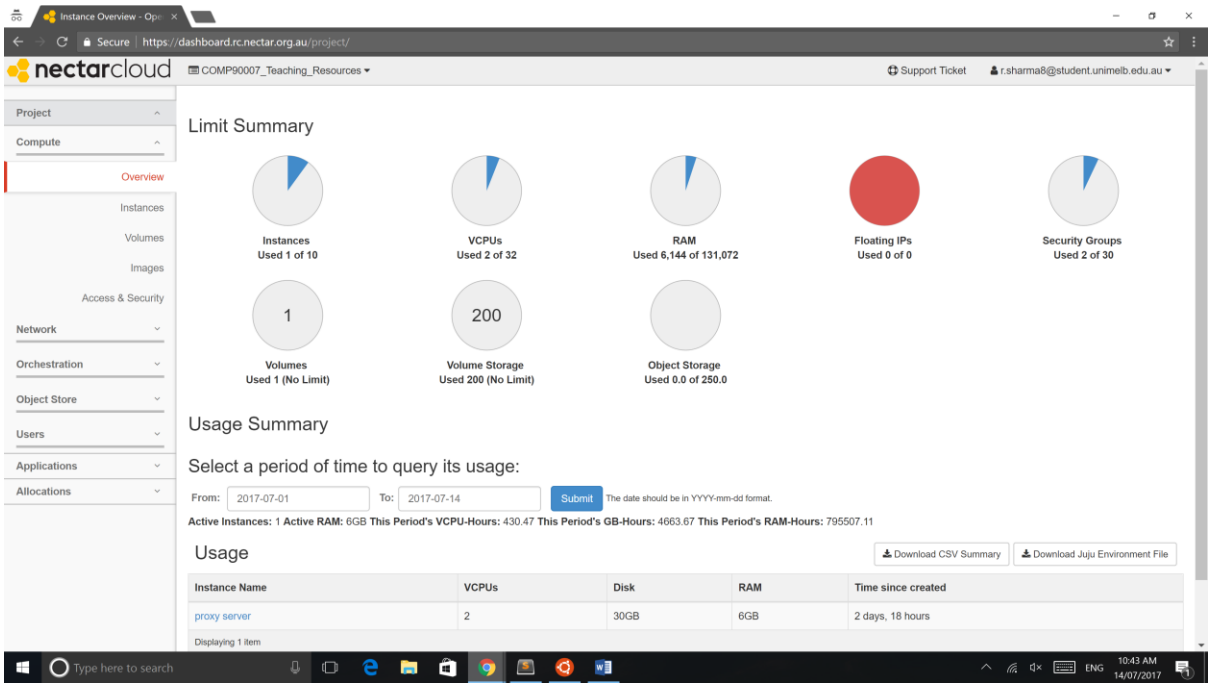


This will lead you to a web page with Unimelb's logo asking for your credentials. Since you are enrolled in the University of Melbourne, you will have an account in their directory so you can directly enter your credentials - username and password (the ones you use to access the LMS) and click on Login.



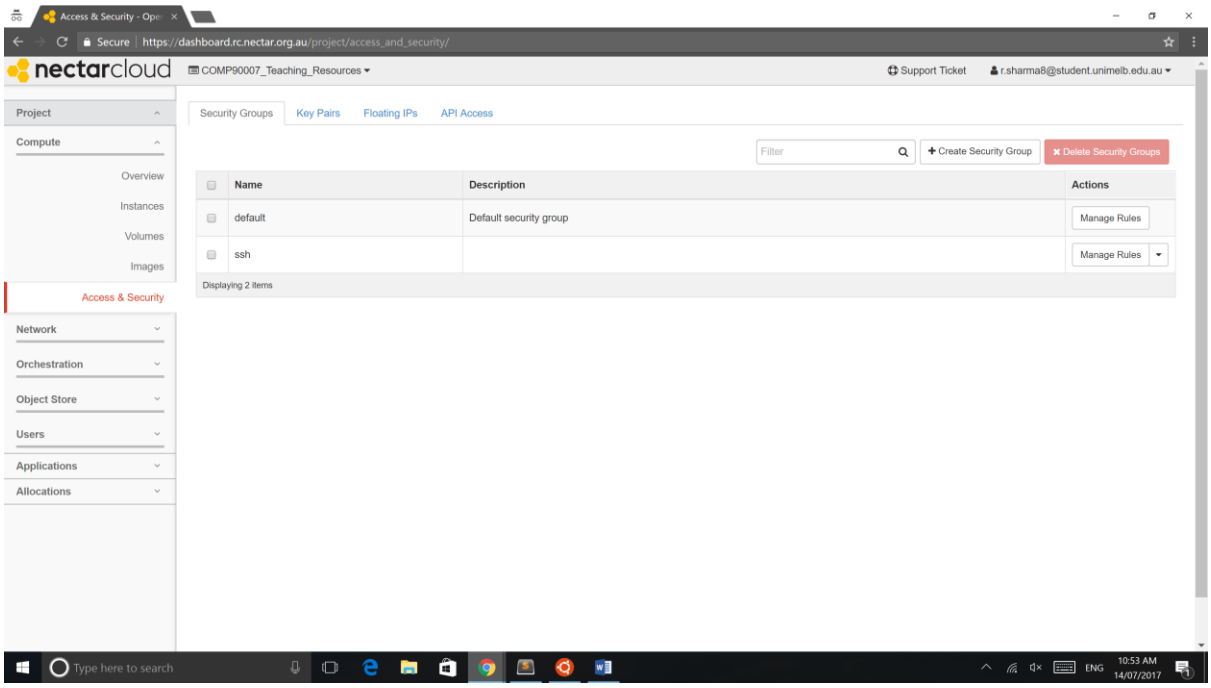
Upon successfully logging in, if this is your first time accessing this platform you will be getting a terms and conditions document. Review it and accept. Upon accepting the terms and conditions document you will have access to the NeCTAR dashboard which looks as seen below.

Deploying a VM

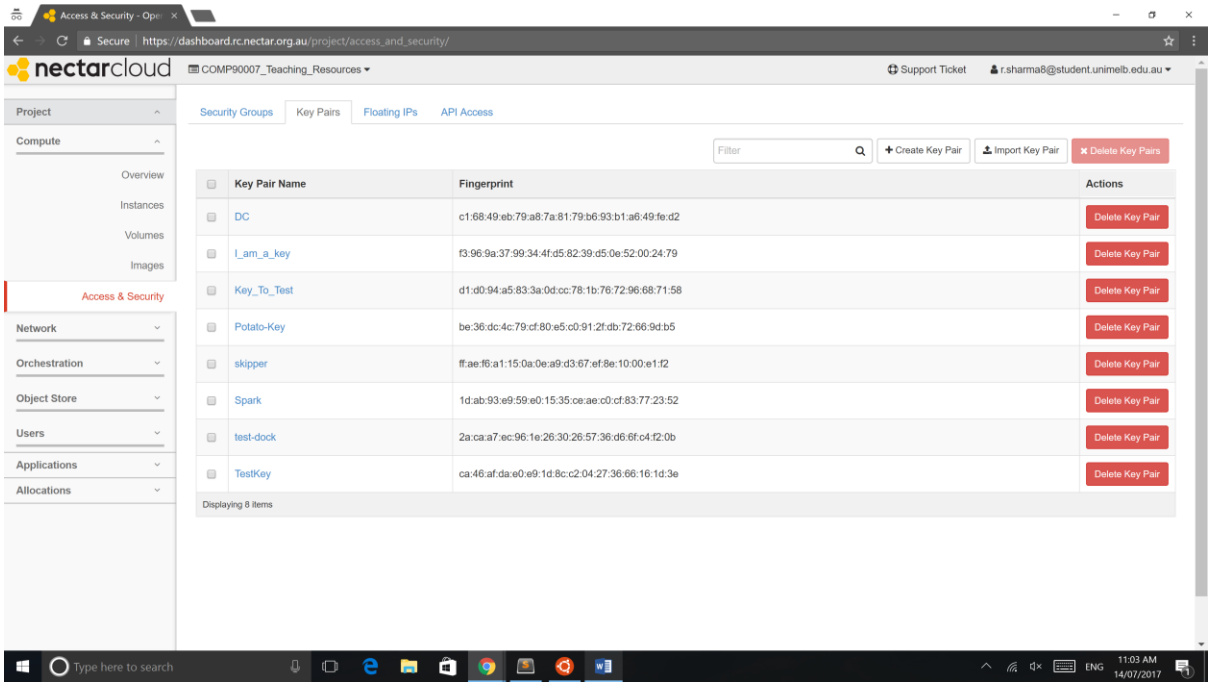


This dashboard reports a few things about the resources available to you. I requested for a few more resources so my dashboard looks a bit different from yours (You do not need to request for more resources for this subject). You most probably will have access to 2 (maybe 4) cores/ VCPUs and 2 VM's, which will be enough to run through this process.

Now Click on the "Access & Security" tab and you will see a dashboard as seen below:

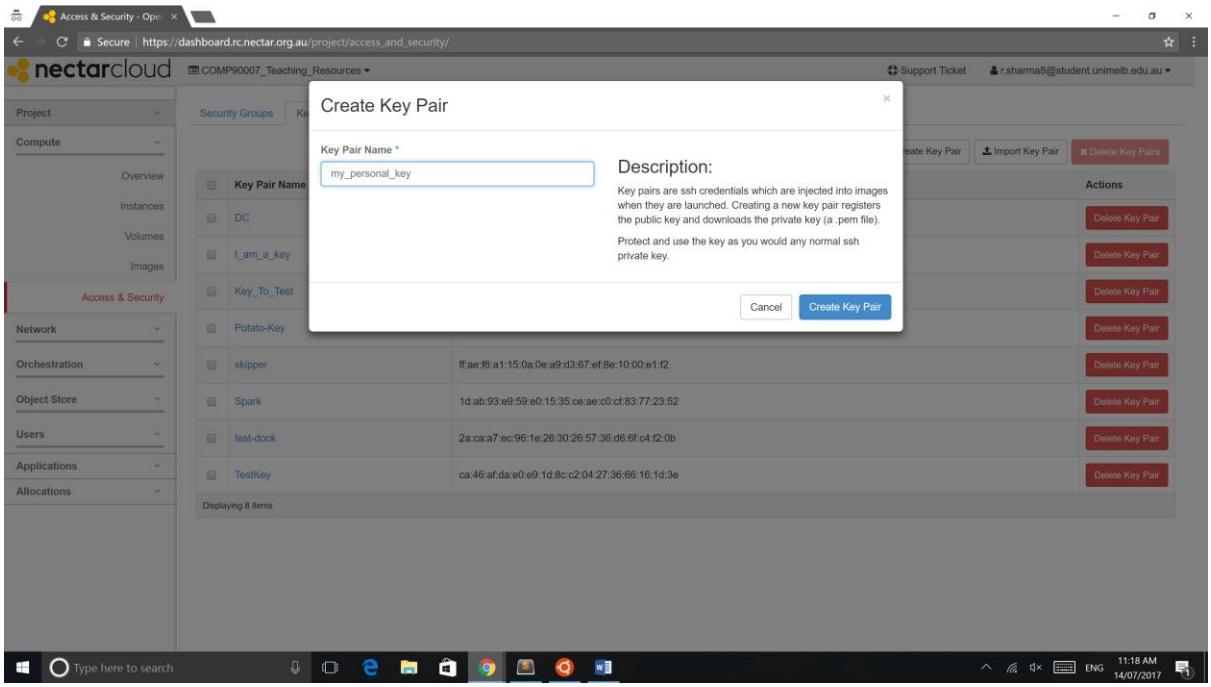


The Security Groups tab would be open by default. You might have a security group called default, I on the other hand created a security group called ssh for myself (for something else) so I have that one extra security group. On the dashboard, click on the key pairs tab.

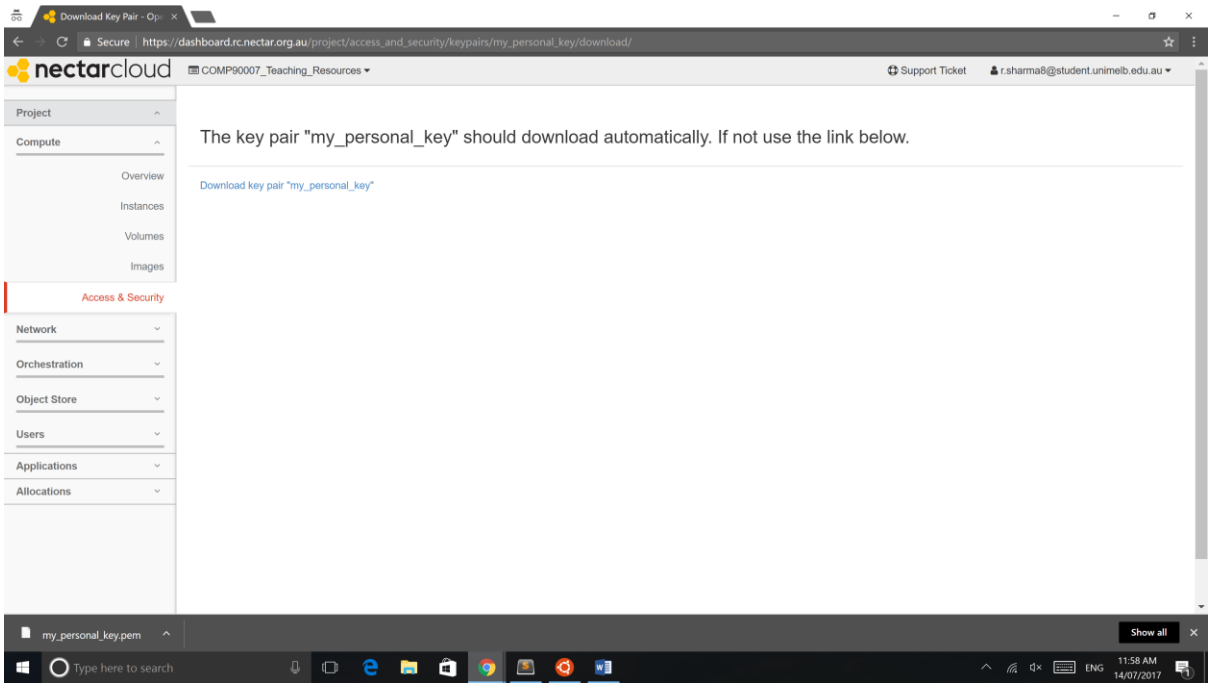


I have a bunch of key pairs available currently as I have been working hard 😉 whereas your dashboard tab should be completely empty.

The first step we take in Deploying a VM (Virtual Machine) is to create a Key pair to ssh (secure shell) into our VM securely (only people who have the matching private key can access it). Click on the "Create Key Pair" button on the top right side of the platform. It will open a pop-up, prompting you to enter a name (human readable) for your key pair. Write a name that you think would be relevant to call your key pair. For example, I named my key pair – "my_personal_key".

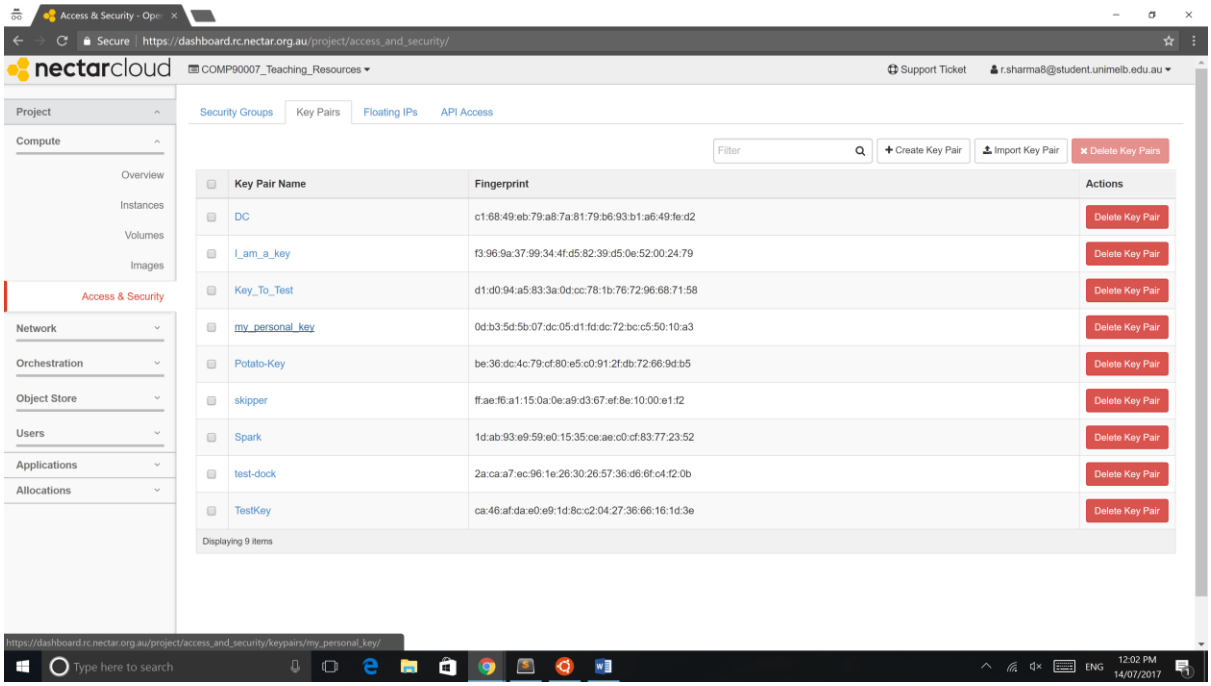


Click on “Create Key Pair”. This will automatically create a Key pair (public-private keys) for you, saving the public key in your account on NeCTAR and downloading the private key onto your personal computer. (**NOTE: The private key can only be downloaded once. Do not lose it because you cannot access your VM without it.**)



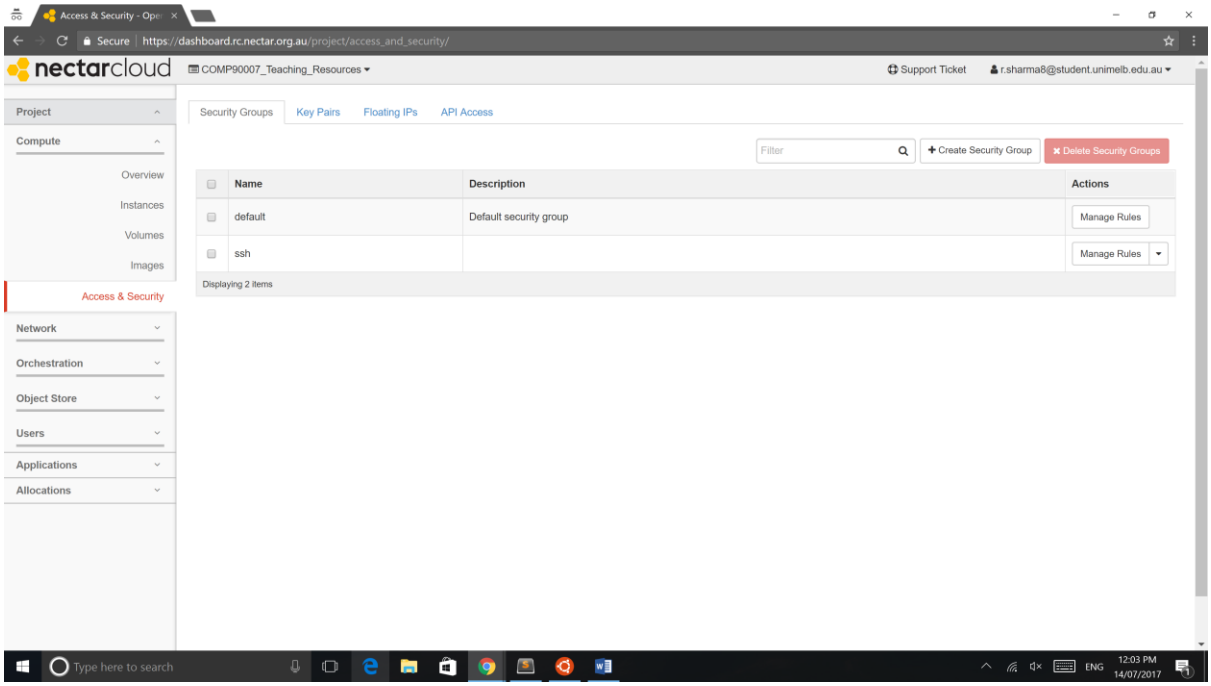
I saved the key on my Desktop in a folder I named “NeCTAR”.

Now, Click on “Access & Security” again and you will be led back to the Key pair page. You will note that the key pair you just created will be visible there (your public is available on the platform). The key I just created – “my_personal_key” is seen in the image below.

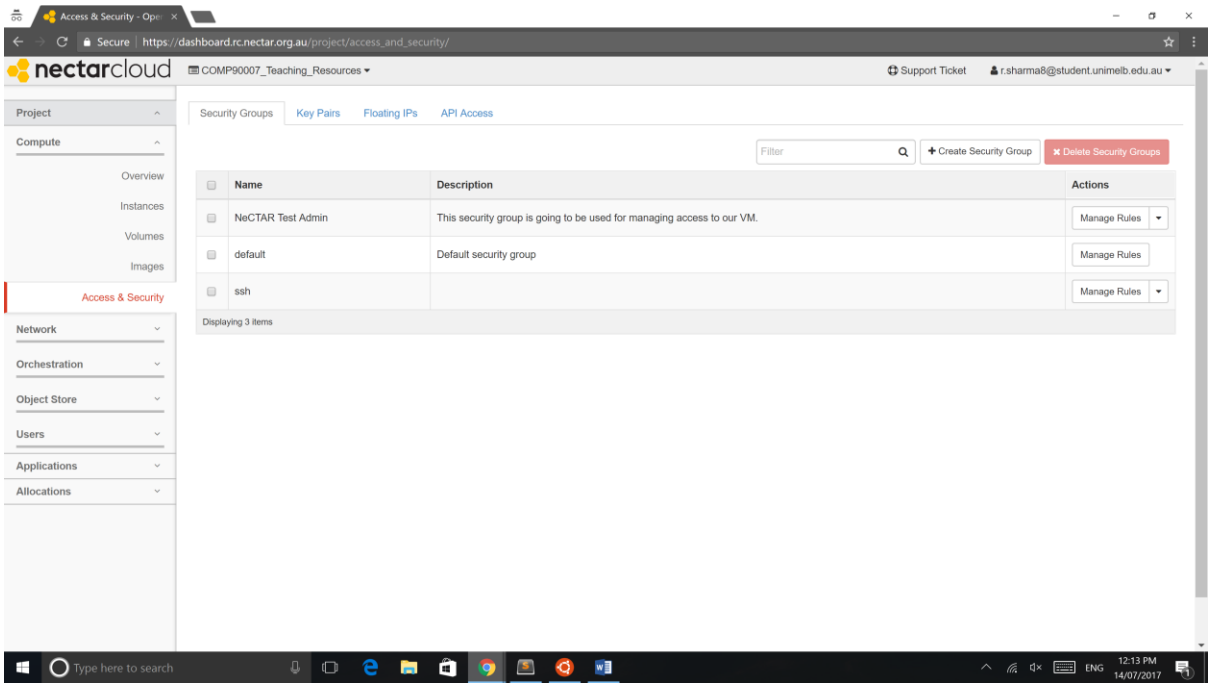


Now Click on Security Groups. You will have a default security group available to you (I have ssh as well that I created). The Security groups section represent Firewalls for the platform. By default, all

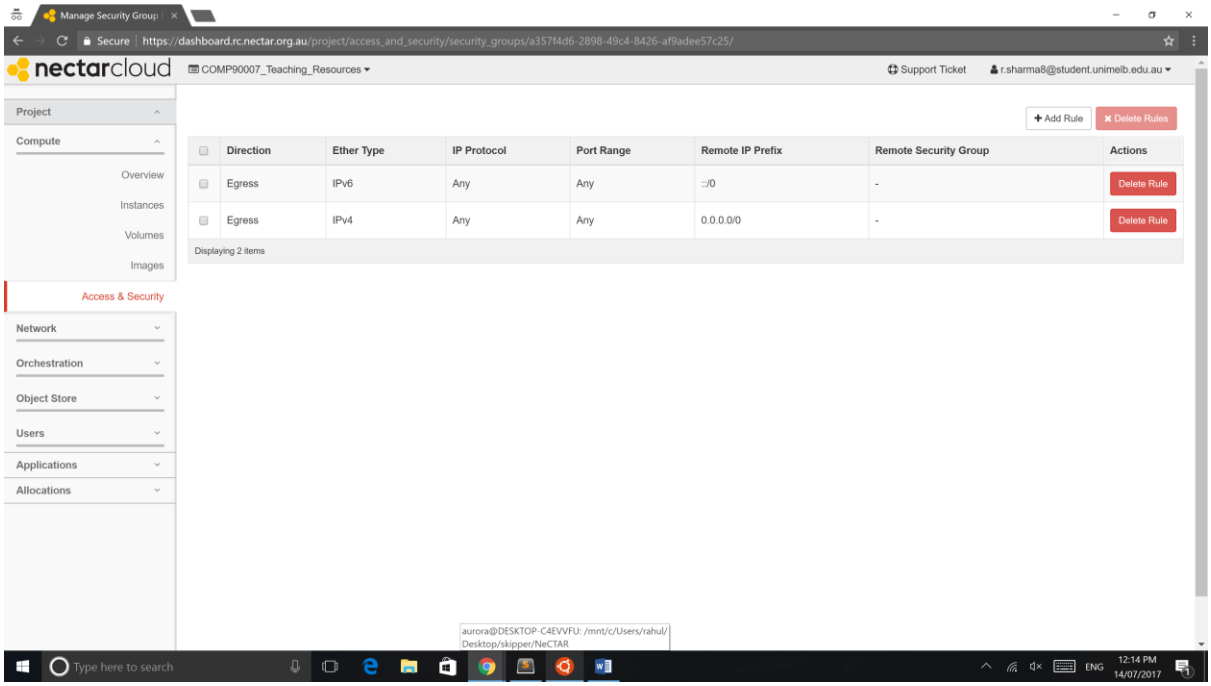
ports (software constructs) are blocked for the compute service on NeCTAR so technically once we create a VM – we cannot do anything. In order to avoid that, we will create a security group for ourselves to be able to access it (using ssh).



For that, click on the button – "Create Security Group". You will be prompted to give a name for your security group with an optional description of the Security Group. I named my security group – "NeCTAR Test Admin". Now click on "Create Security Group". Your security group will be created and made visible on the platform.

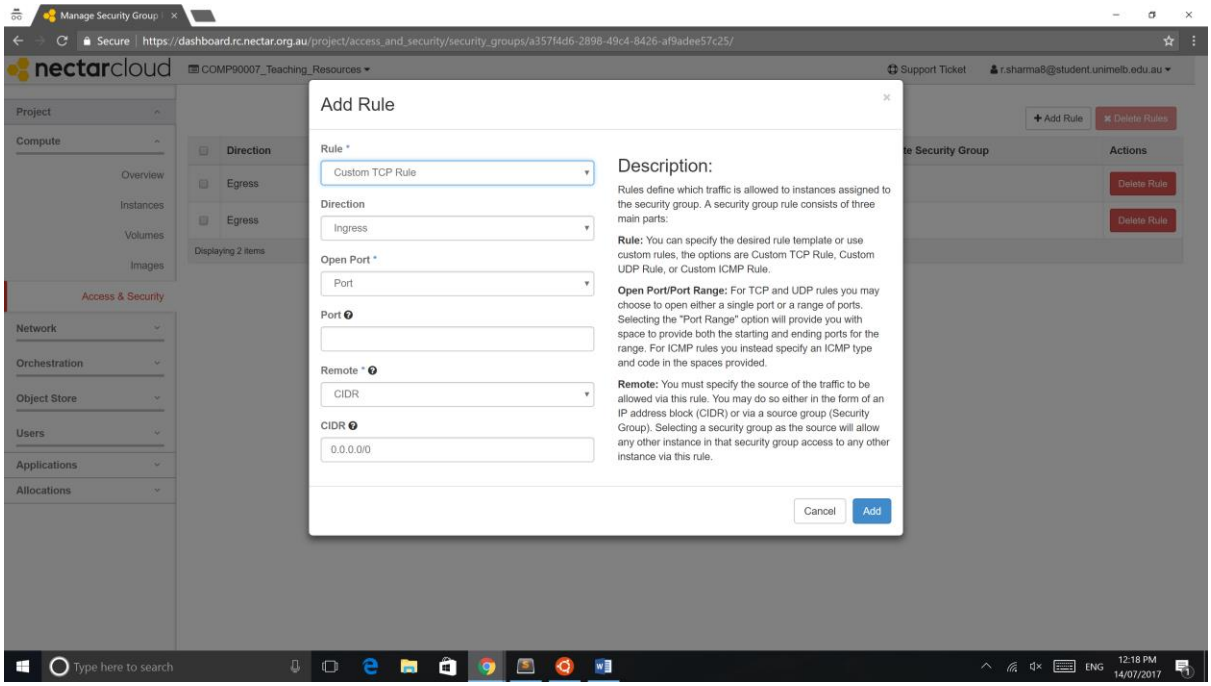


Click on the button – "Manage Rules" for your newly created Security Group (for me its – NeCTAR Test Admin" and you will be led to a page as shown below.

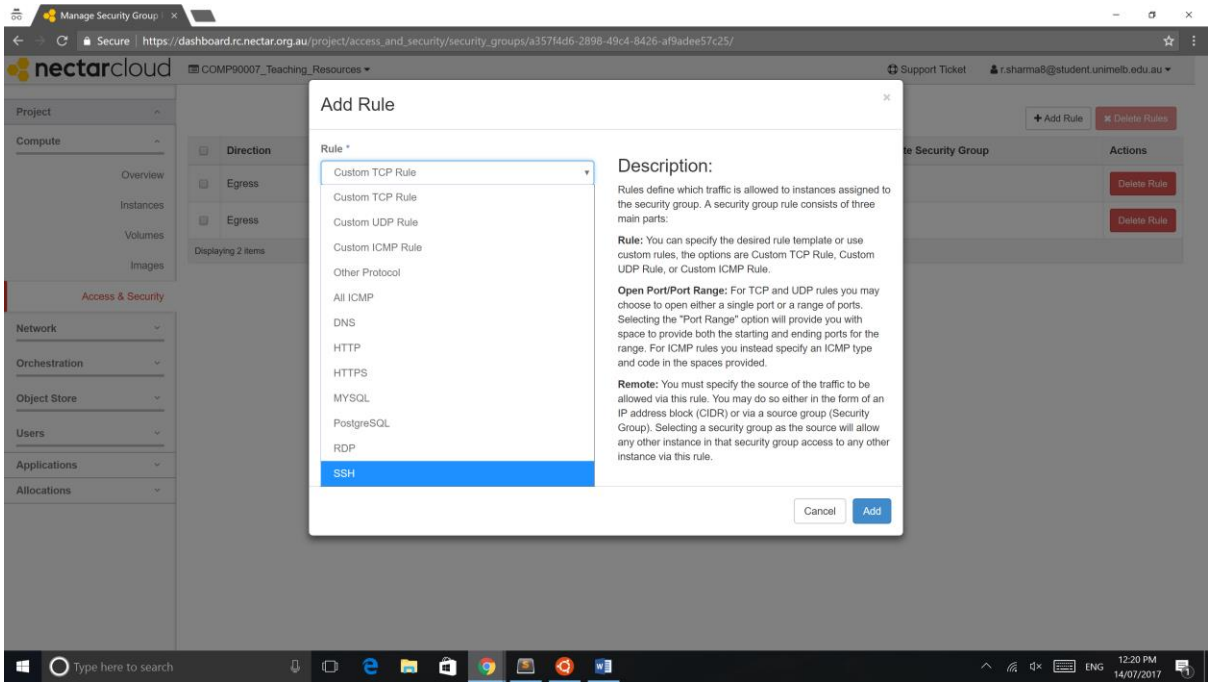


This page shows all the ports that are open at present and whether its bound to a particular IP address. The first thing we need to do here is to enable ssh to be able to access our VM. If we do not enable ssh, we will not be able to access the VM.

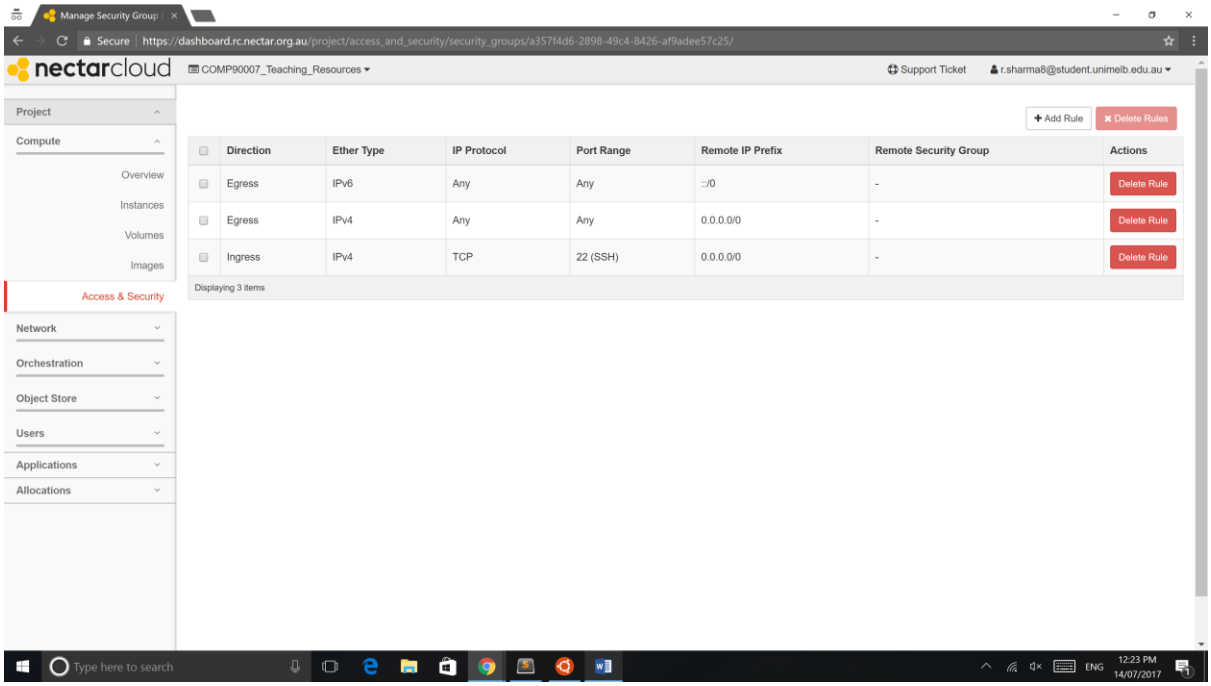
To open up the port for SSH, click on – “Add Rule”. This will open up a pop-up asking what type of protocol would you like to allow that too at what port, allowing a given IP address or rather addresses.



Since I want to enable ssh, I click on the drag down menu for Rule and choose SSH.

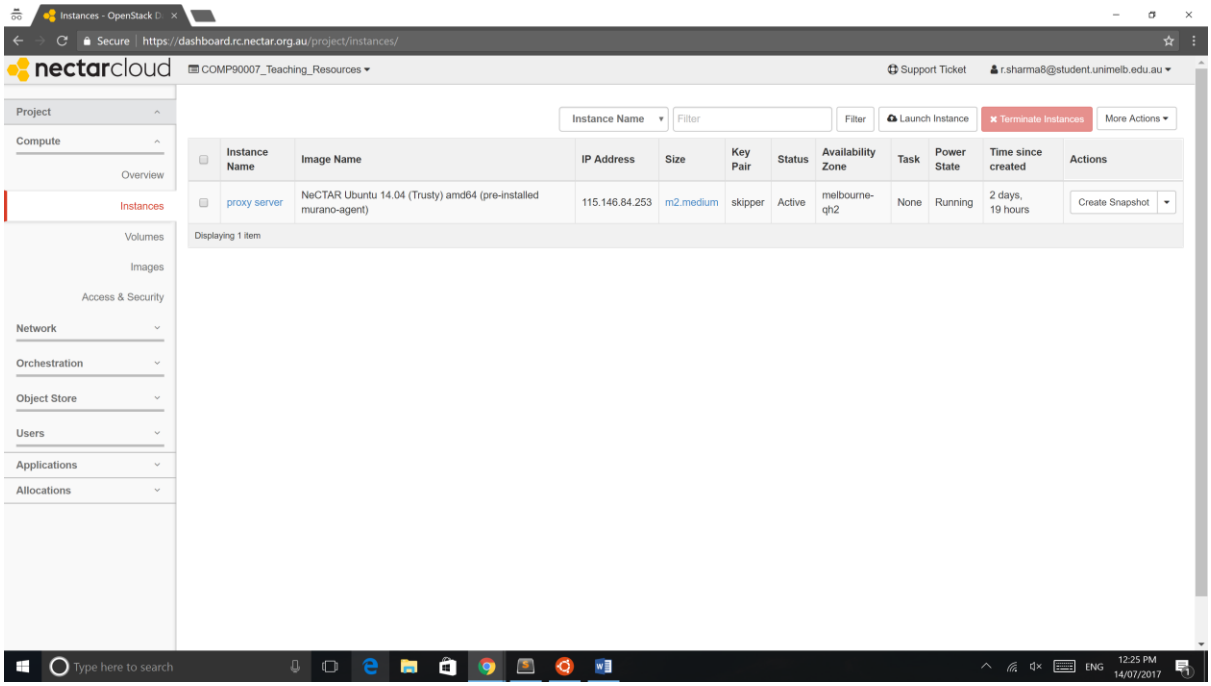


I will leave the rest of the parameters as it is (CIDR – Allow Classless Inter Domain Routing with a default route available, allowing all IP addresses to access it) and click on “Add”.



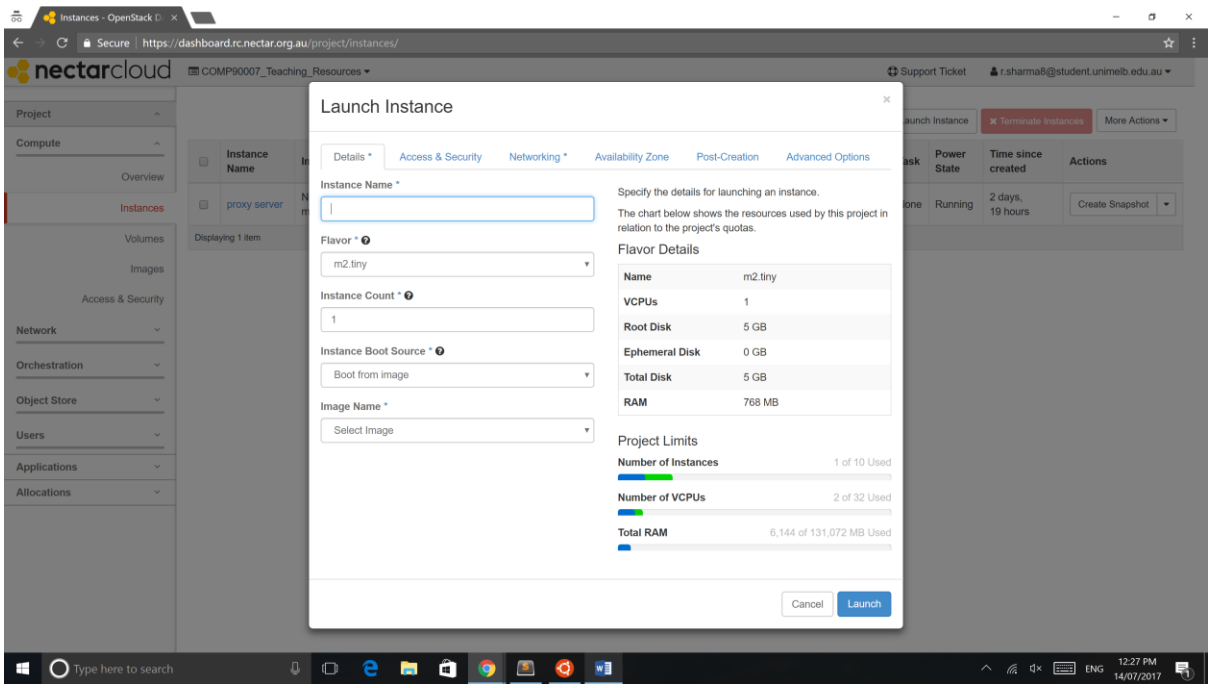
This will open up port number 22 (for ssh) which will allow you to access a given VM using that Security Group through the use of your key.

Now Click on the “Instances” tab on the left pane of your dashboard. You will see a screen as shown below.

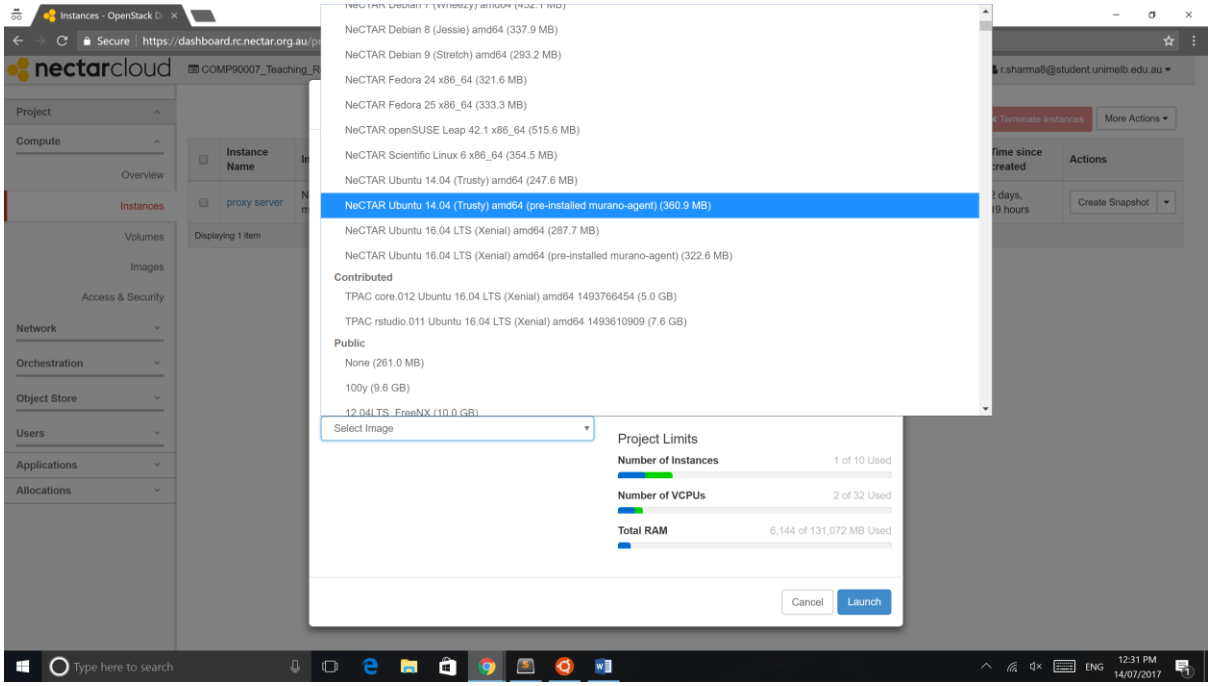


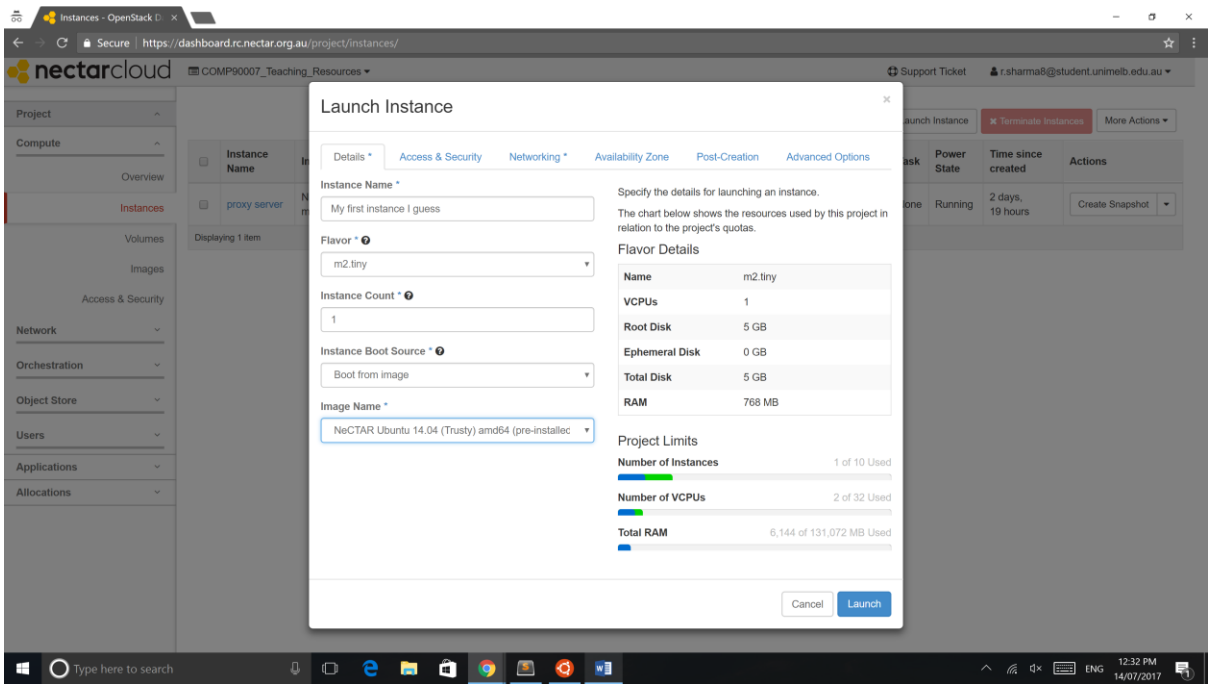
Your screen will not show any VM's (mine does because I am working on something).

To launch a VM, click on "Launch Instance" on the top right hand corner of the dashboard. You will be shown a pop-up asking you to enter details and choose the type of configurations your VM needs to have.

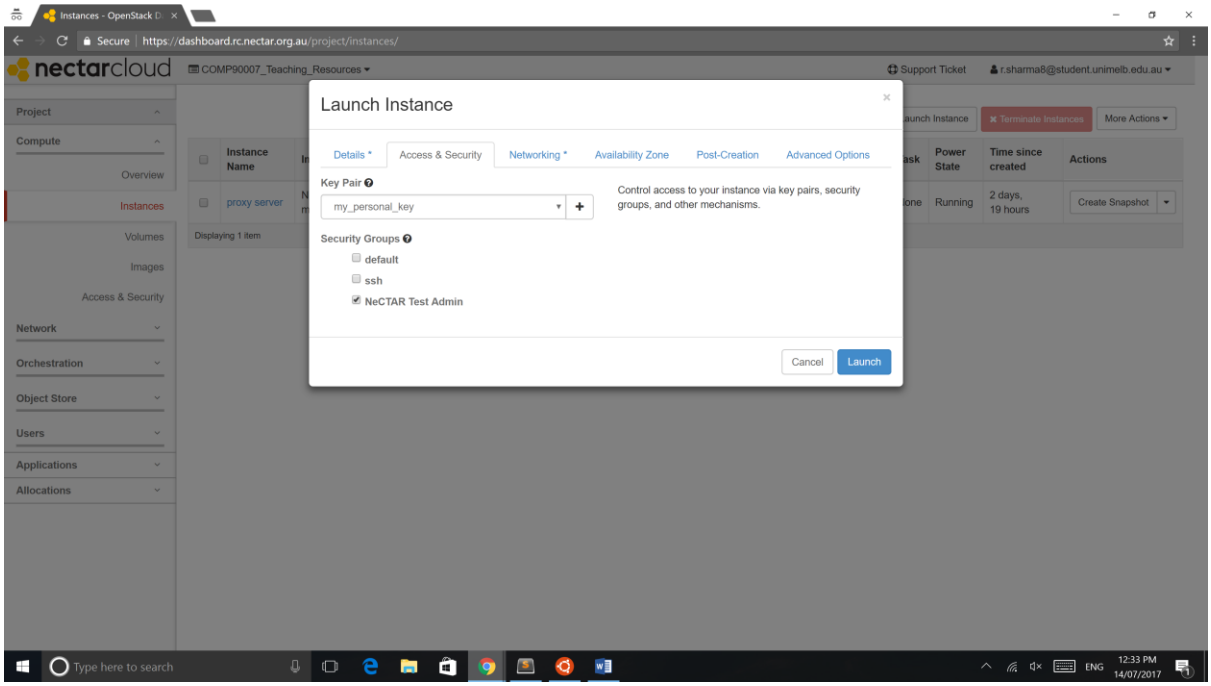


Start by naming your instance as what you feel is relevant. Choose a flavor of the VM, right now pick m2.tiny because your resources will be limited by default. Do not change the "instance count" or "Instance Boot Source". For Image name, its about picking an OS that you want your VM to have. I prefer Ubuntu 14.04, so I click on the drag down menu for it and locate that particular image.

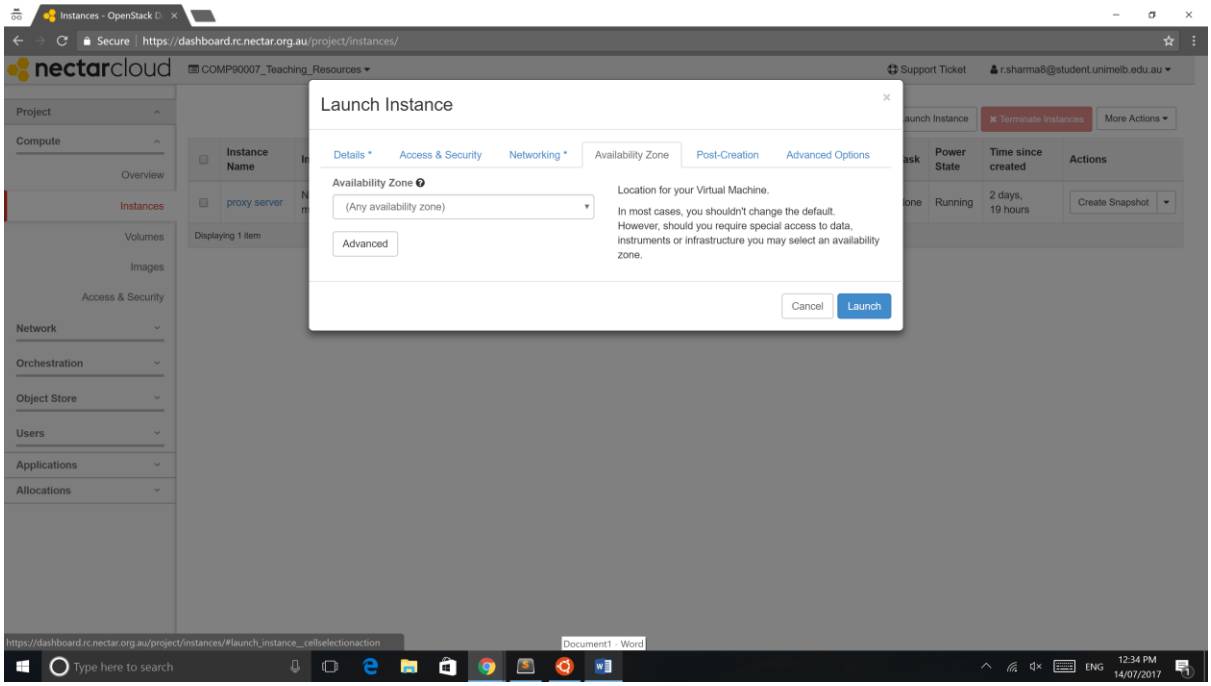




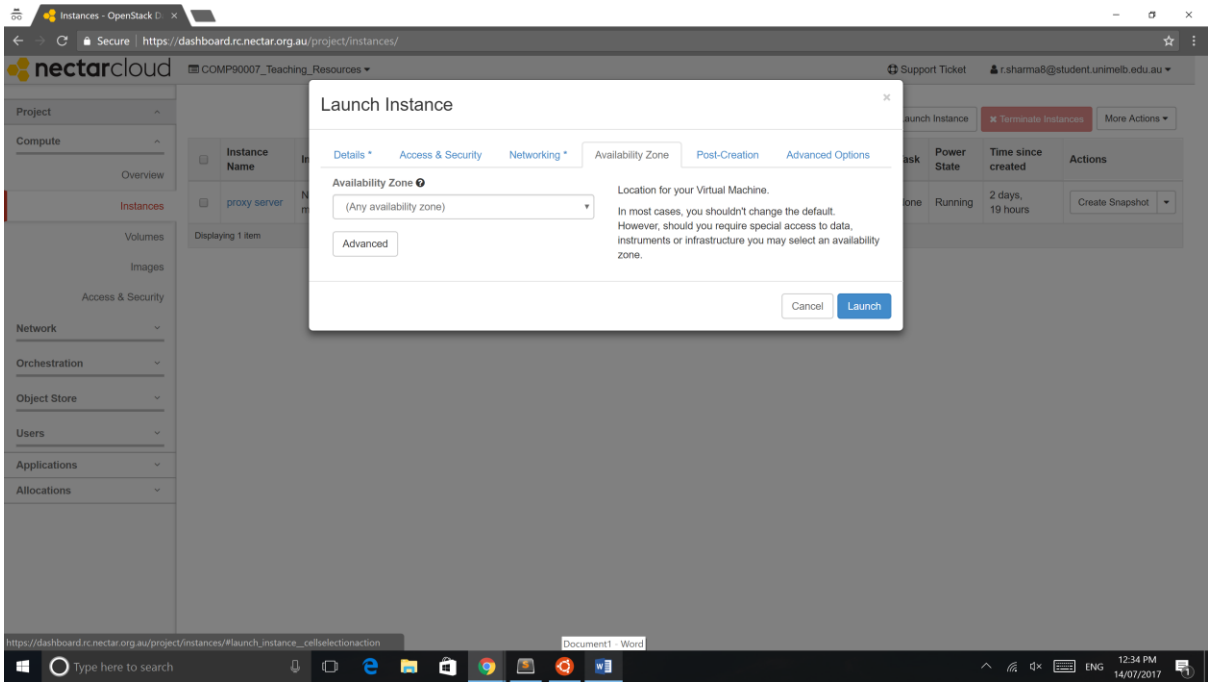
Now Click on the “Access & Security part of the pop-up and select your Key pair (I created my_personal_key so I chose that) and your security group (I am picking NeCTAR Test Admin).

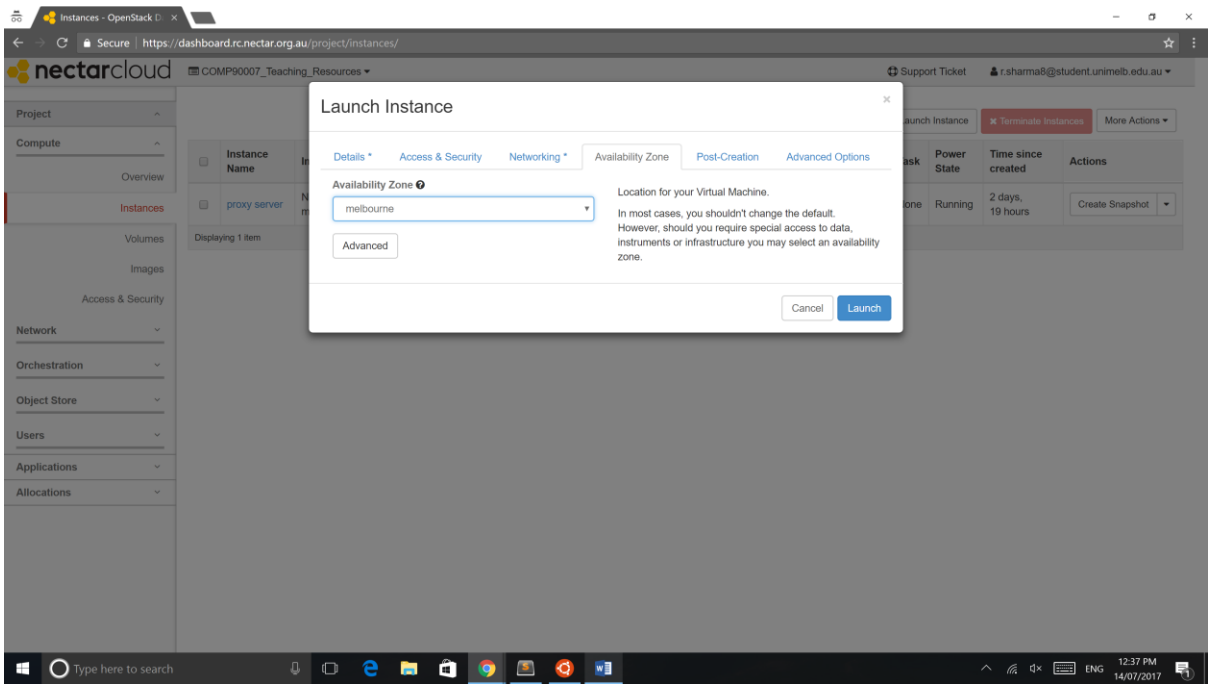


Now Click on the “Availability Zone” tab of this pop-up.

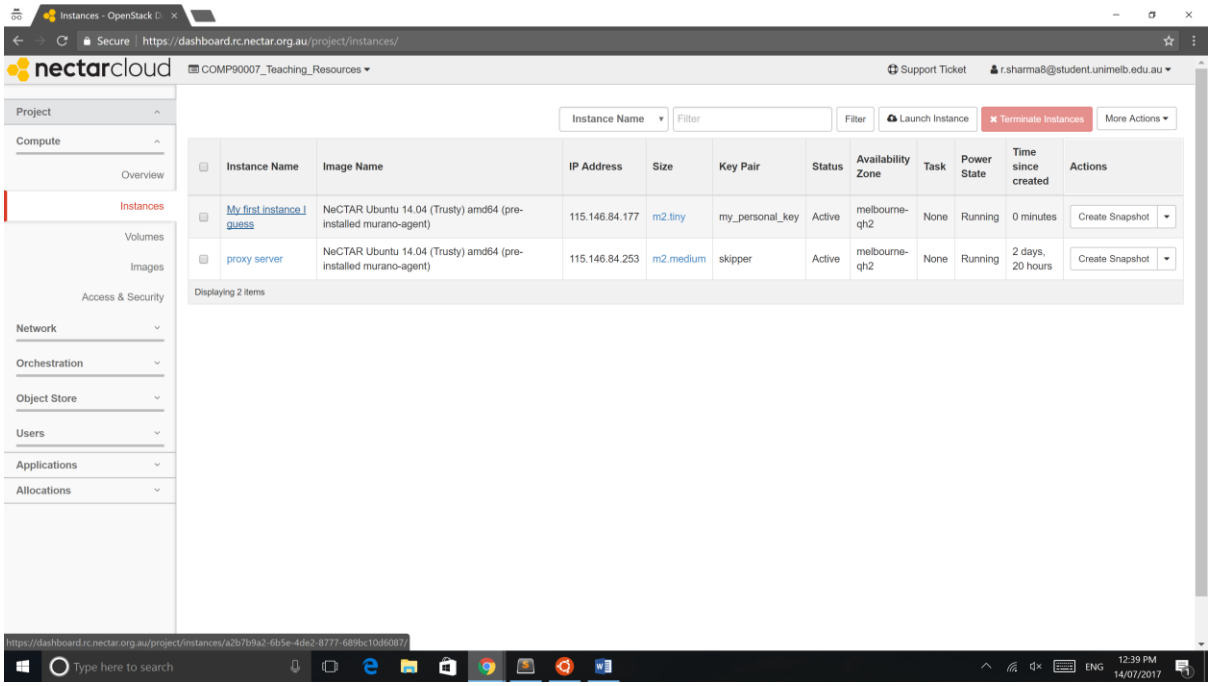


Availability zones specify where (geographical location) you are deploying your VM. I am picking “Melbourne”





Finally click on “Launch”. This will start the deployment process of your VM in the Melbourne Data centre. Upon a successful deployment, you should be able to see an IP address being displayed for your VM. This is a public IP address that is connected to the public network (the Internet) which will be used to ssh into the VM.



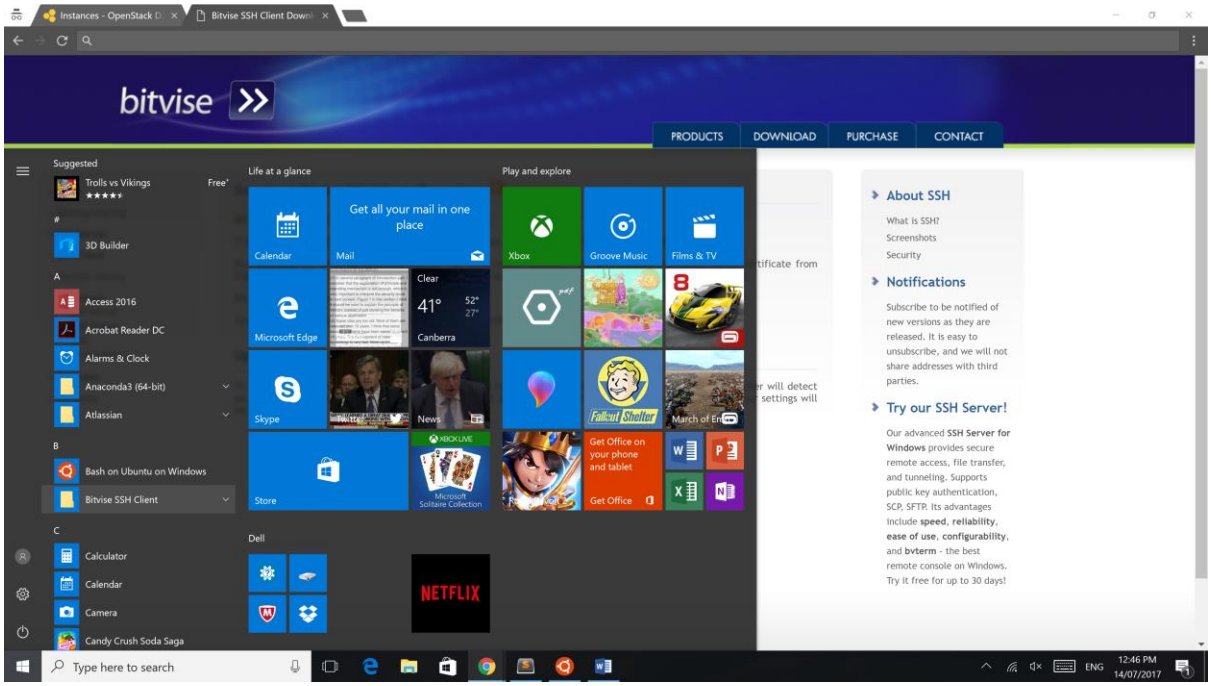
Now that we have deployed a VM, we need to try and access it. To be able to do this, we will use definitive steps to be able to access it using your Windows or Unix/ Linux based (like Mac OSX) system.

Accessing your VM

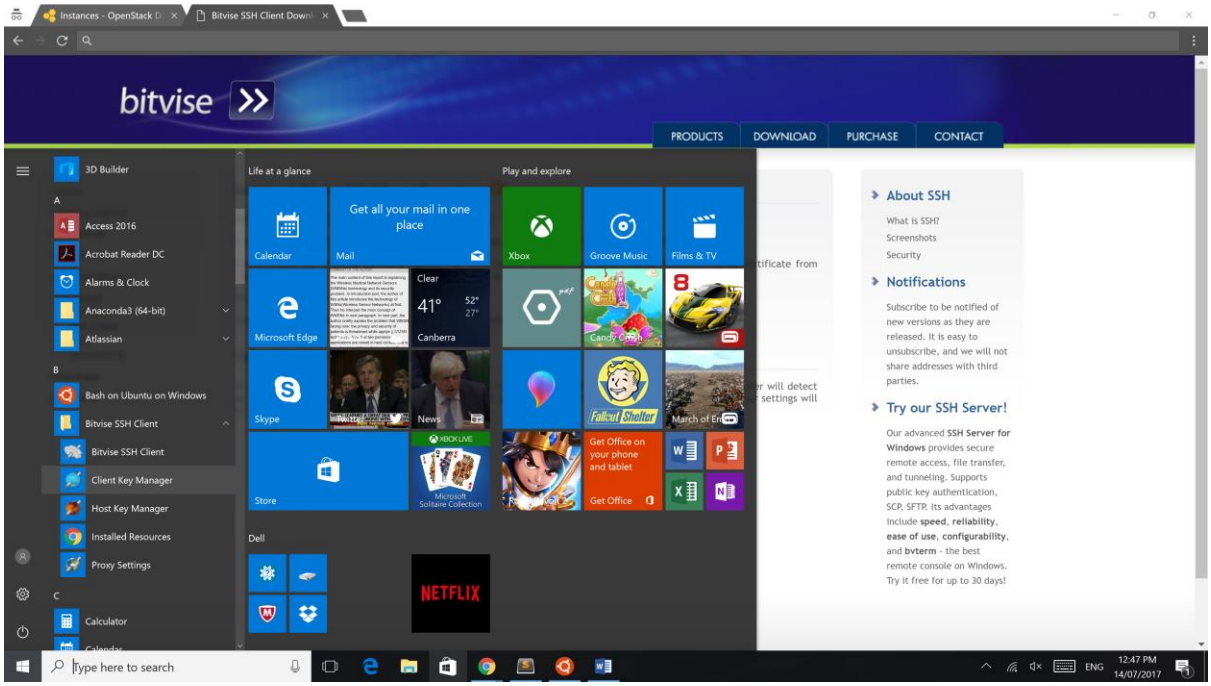
For Windows:

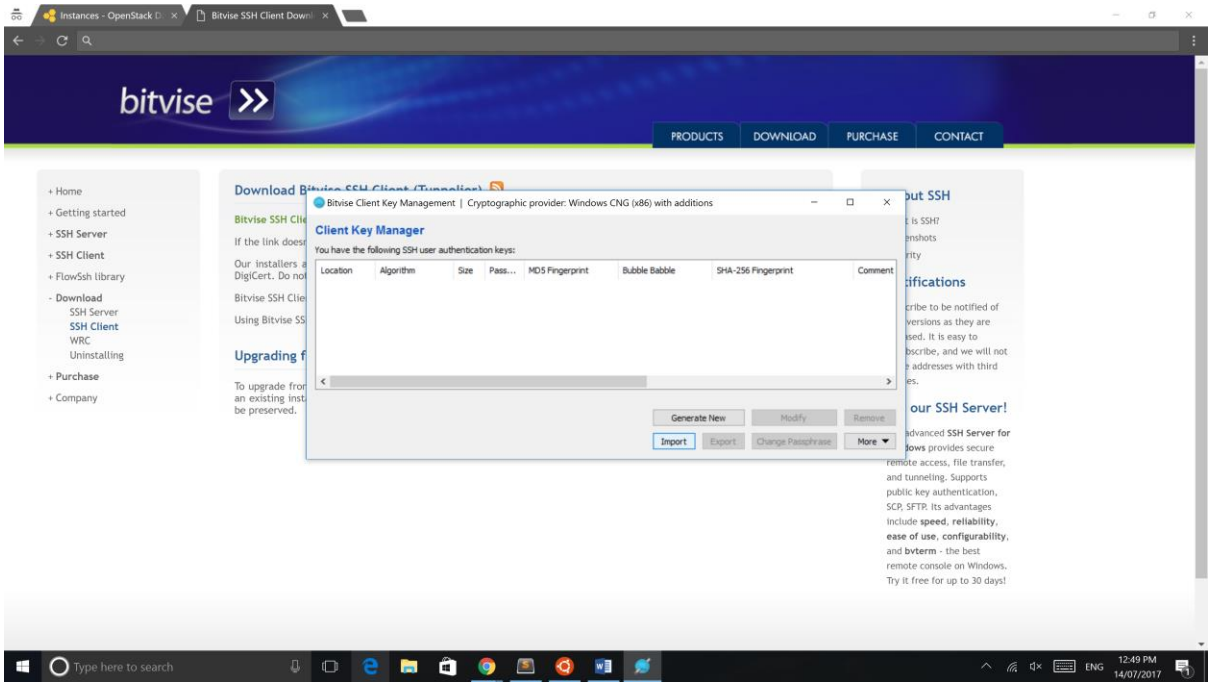
I am going to use a software called bitvise ssh: https://www.bitvise.com/ssh-client-download

Download the client and install it onto your computer. Now click on the start menu of your desktop and locate the folder for bitvise ssh under the alphabet "B"

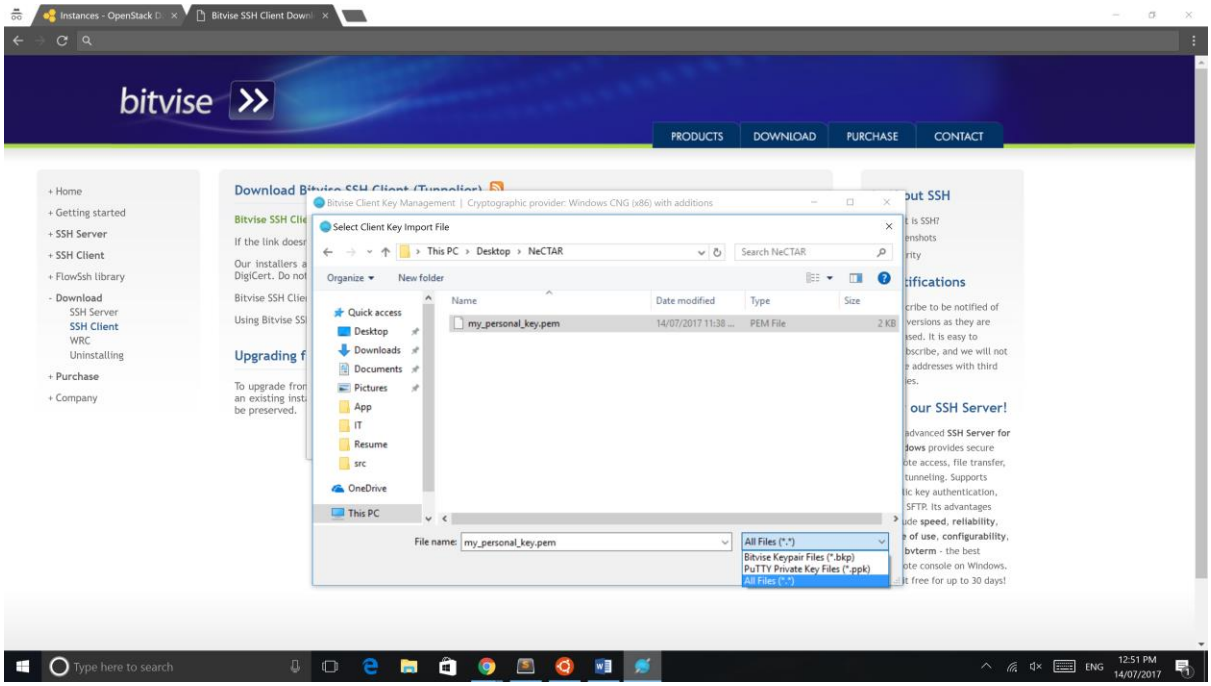


Open the folder and click on Client key manager.

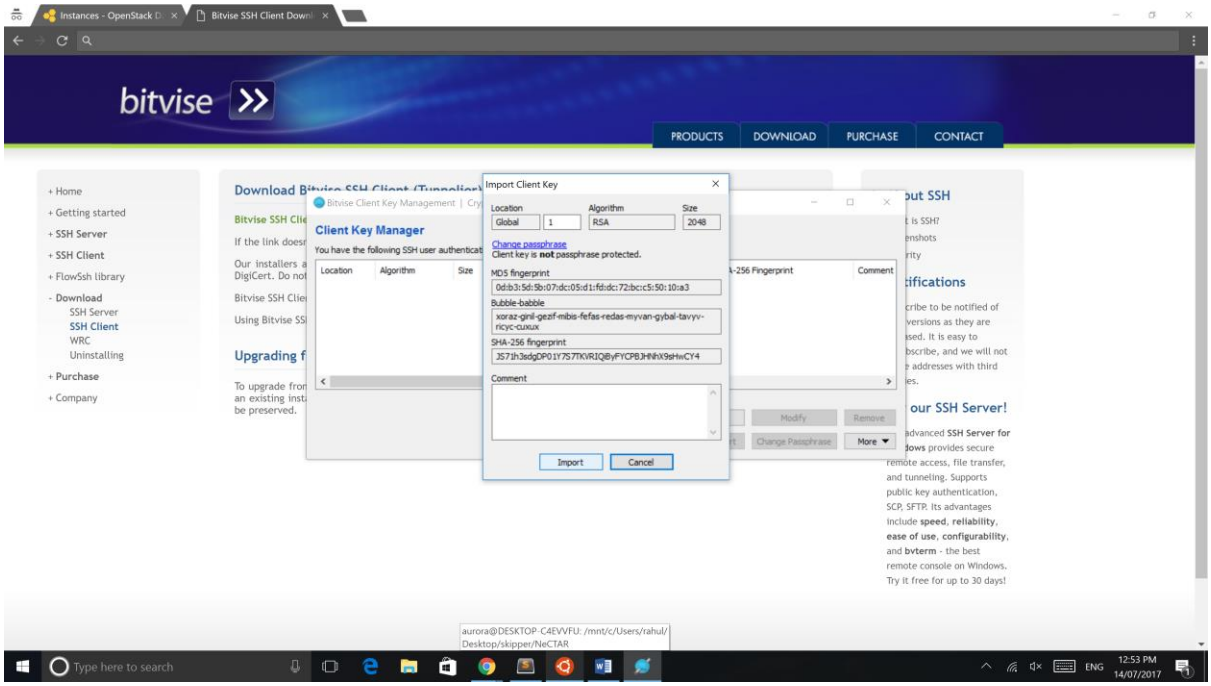




Click on “Import” and locate the place where your key is stored. Since we are using a .pem extension for the file, we need to choose the “All Files” option in the window.

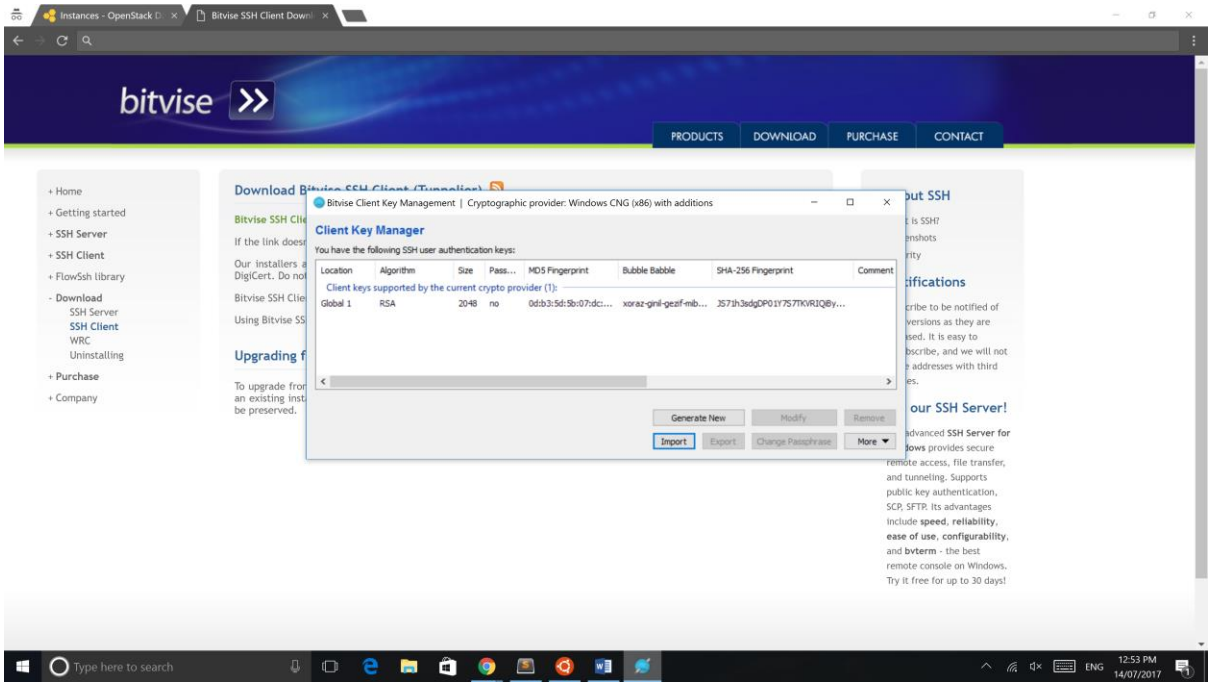


Choose your key and select “Open”. You will see a screen as below.

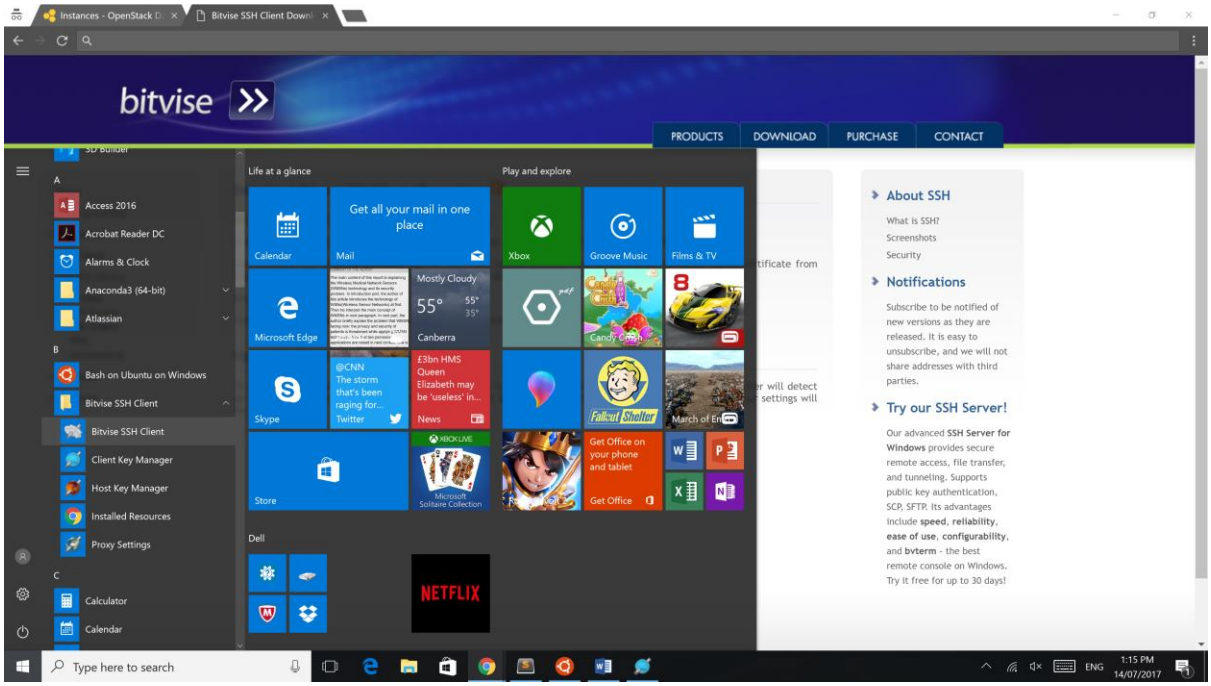


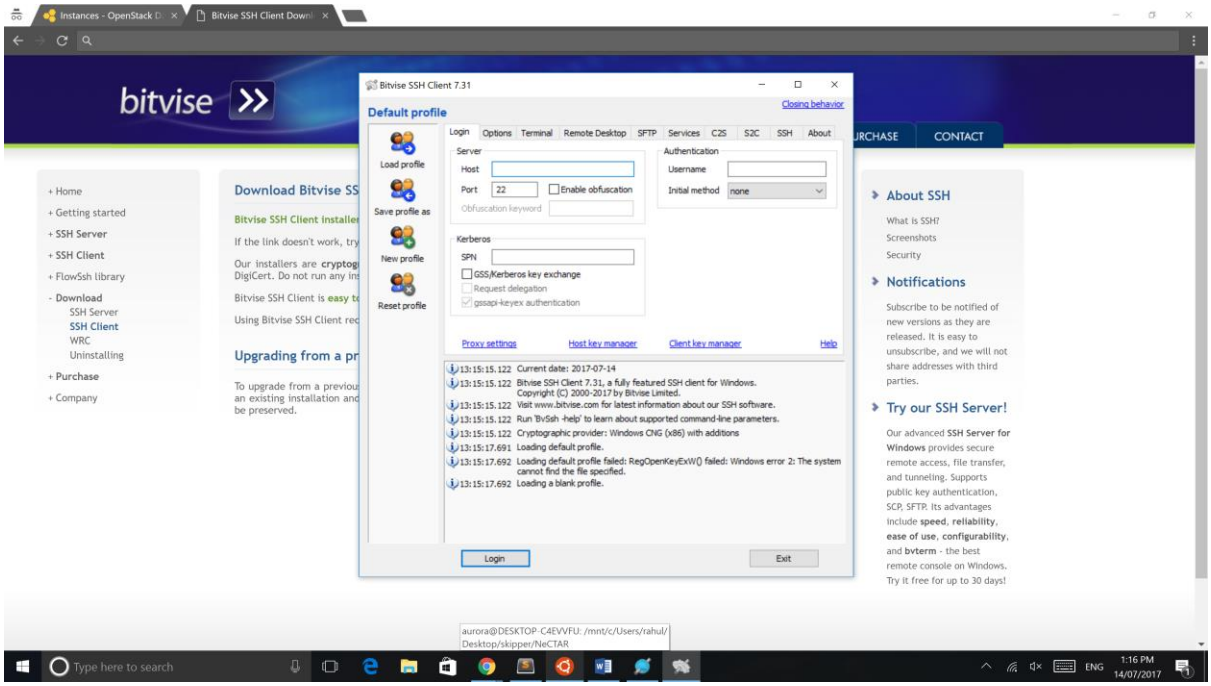
Click on “Import”.

You will now notice that the key has been registered on Bitvise and is referred to as “Global 1”.

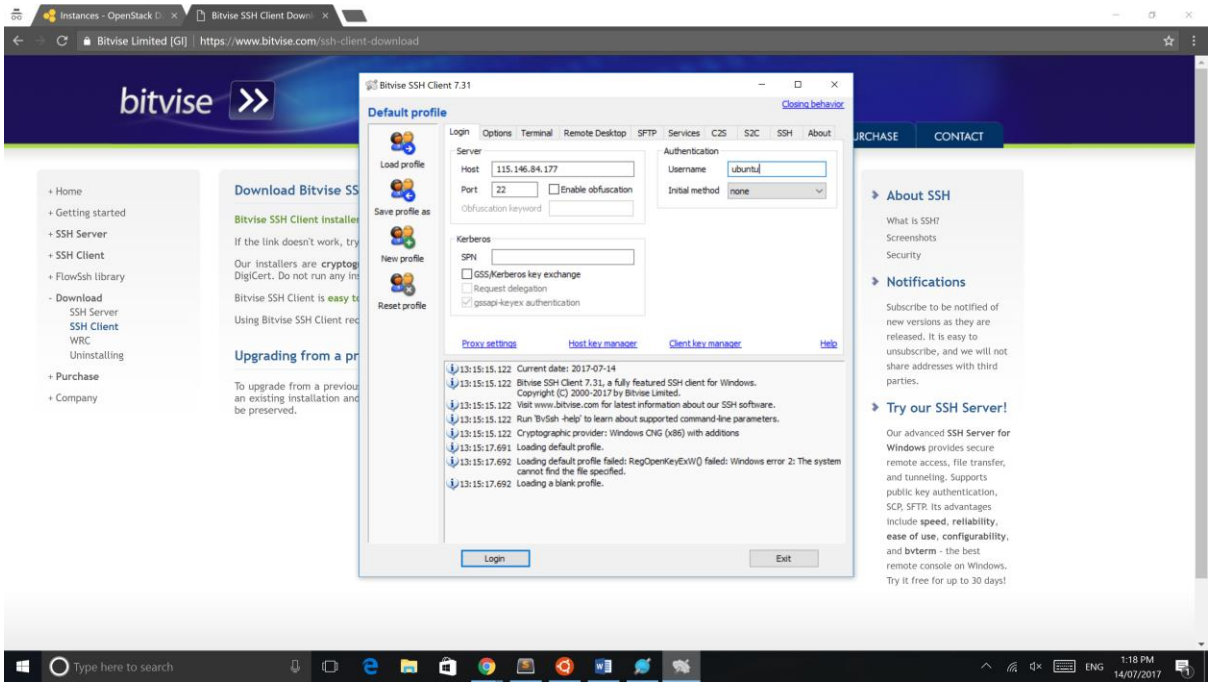


Now go back to the start menu and find the Bitvise folder. Open the folder and choose “Bitvise SSH Client”

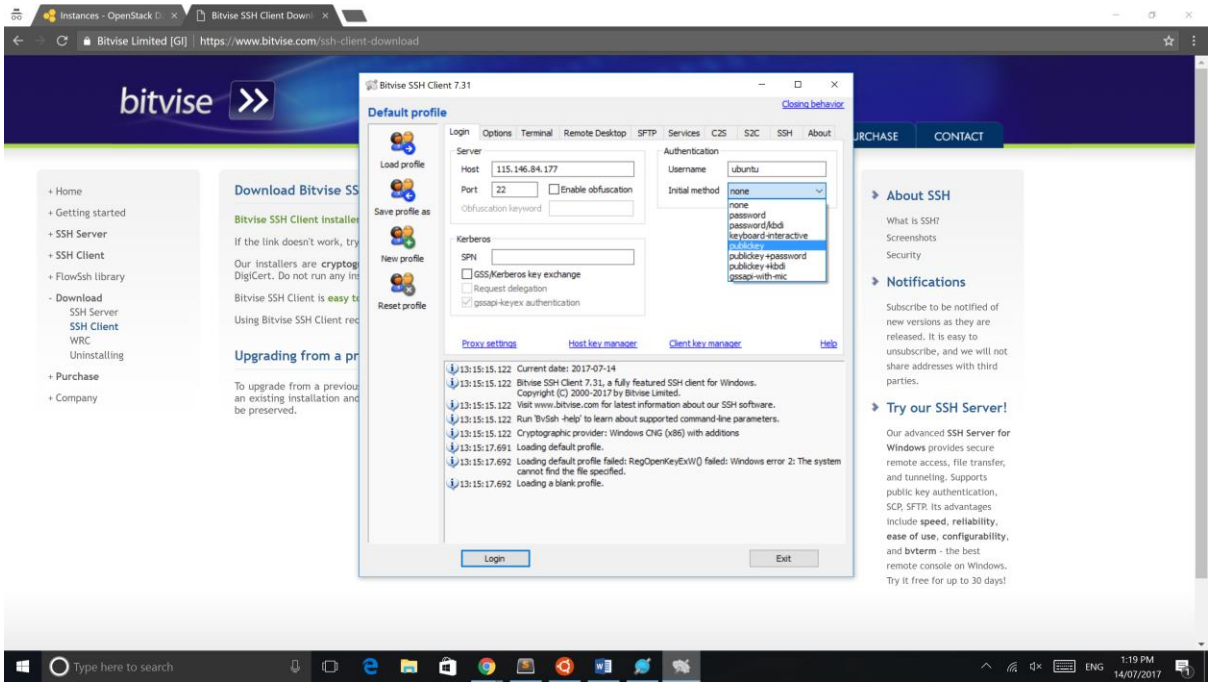




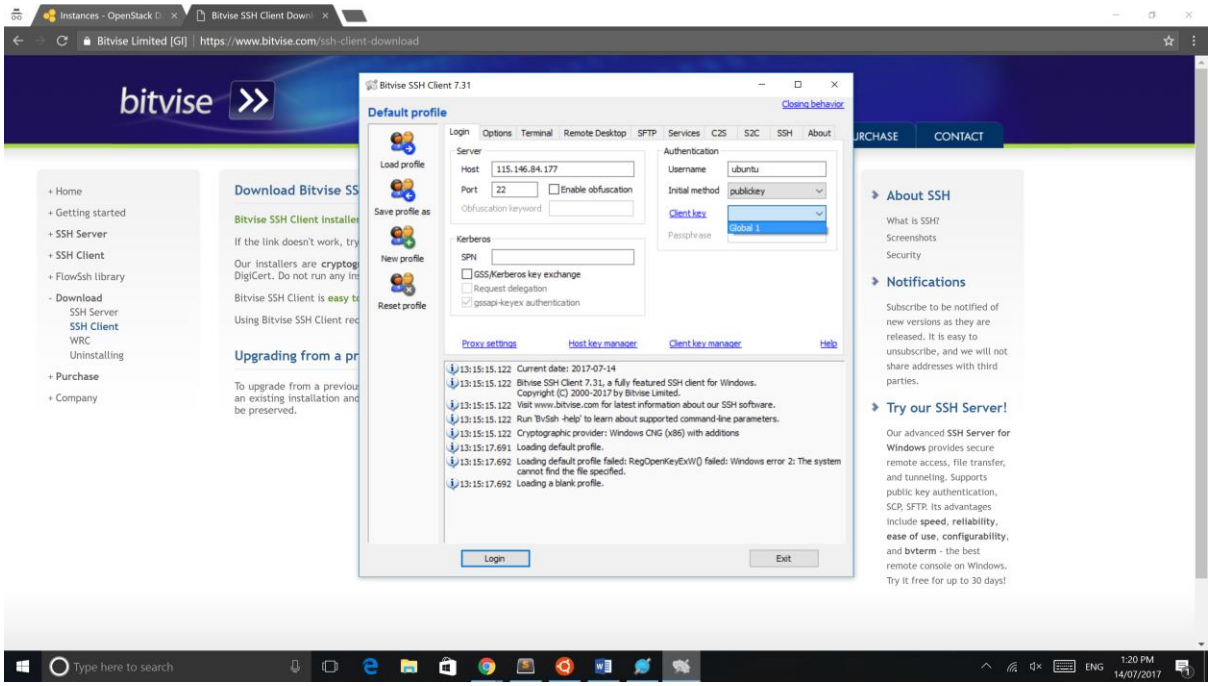
In the host part, enter the IP address as given on the NeCTAR dashboard for your newly created VM. For me, it was “115.146.84.177”. Leave the port on 22 (SSH). For username, type: “ubuntu”.



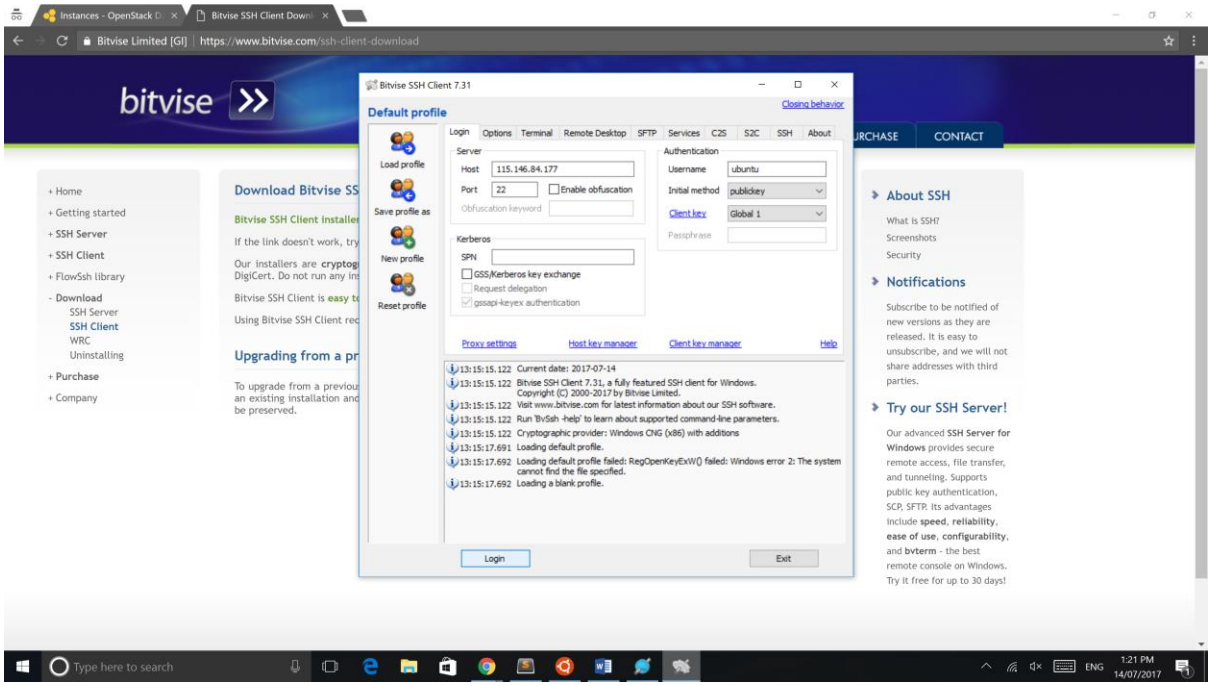
In Initial method, choose: publickey.



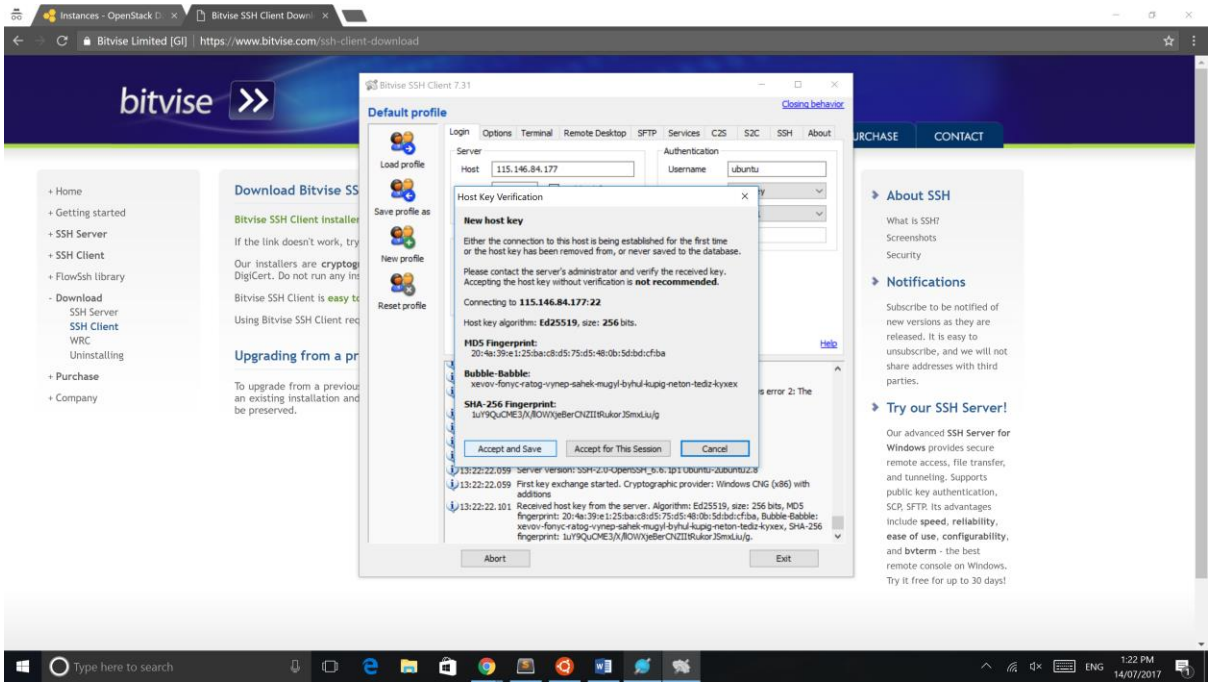
You will see a “Client Key” option now. Click on the drag down menu and choose Global 1, which was the reference name saved for your key when uploaded to the Client Key Manager on Bitvise.



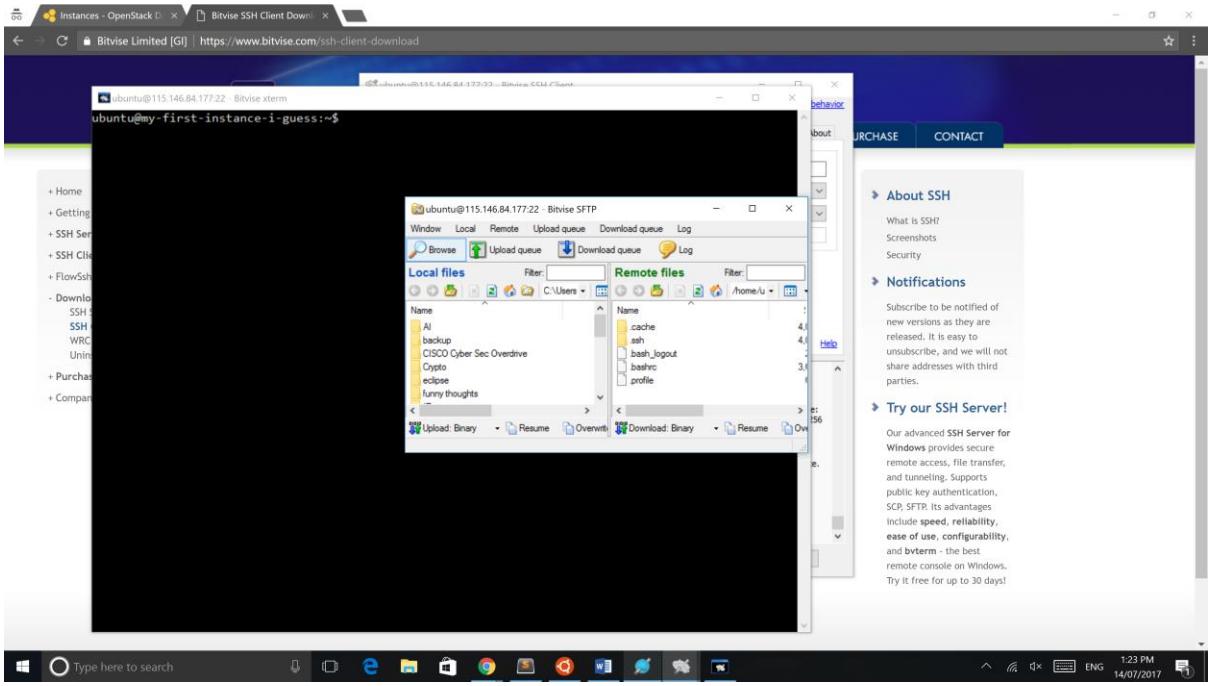
Now that everything is selected, click on “Login”



Since this is the very first time we are trying to access this VM using this key on Bitvise, we are going to be prompted to save the signature. Click on “Accept and Save”.



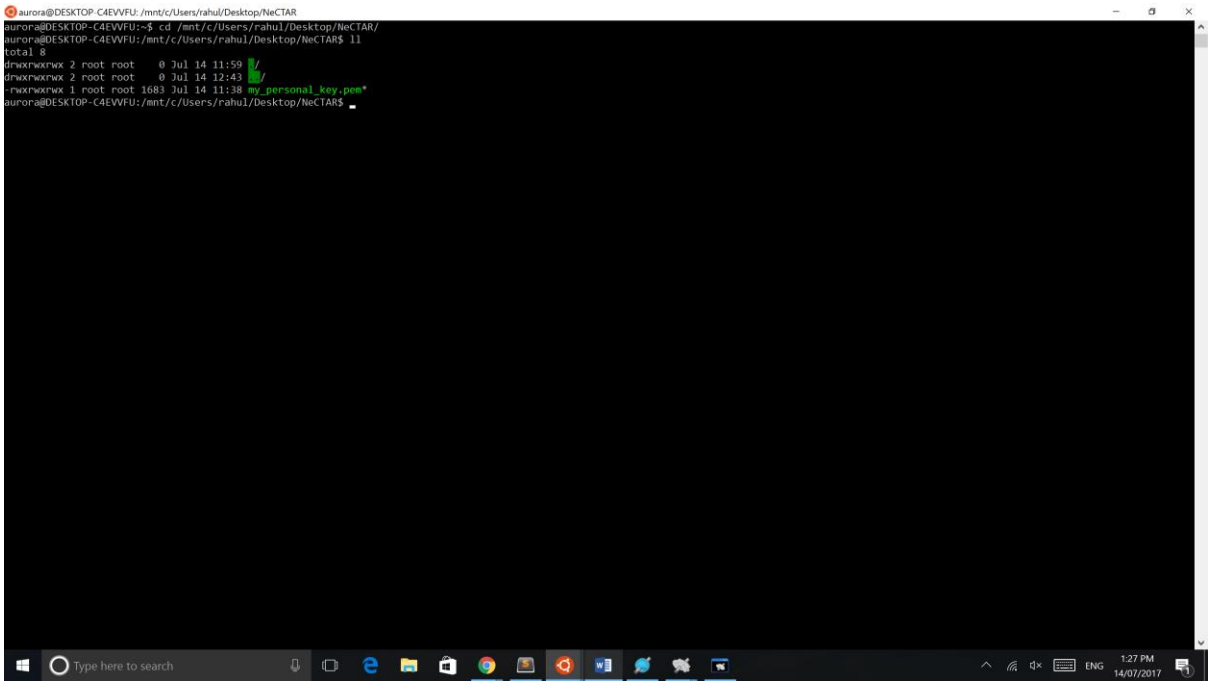
As soon as you click (before timeout… if you don’t click accept quickly, it will time out. Click on Login again if a timeout happens) on that, you will see a terminal pop open along with a window detailing your directory structure (local as well as the one for the VM).



Congratulations! You have accessed a remote VM using your windows machine \(^.^)/.

For Unix/ Linux (Mac OSX):

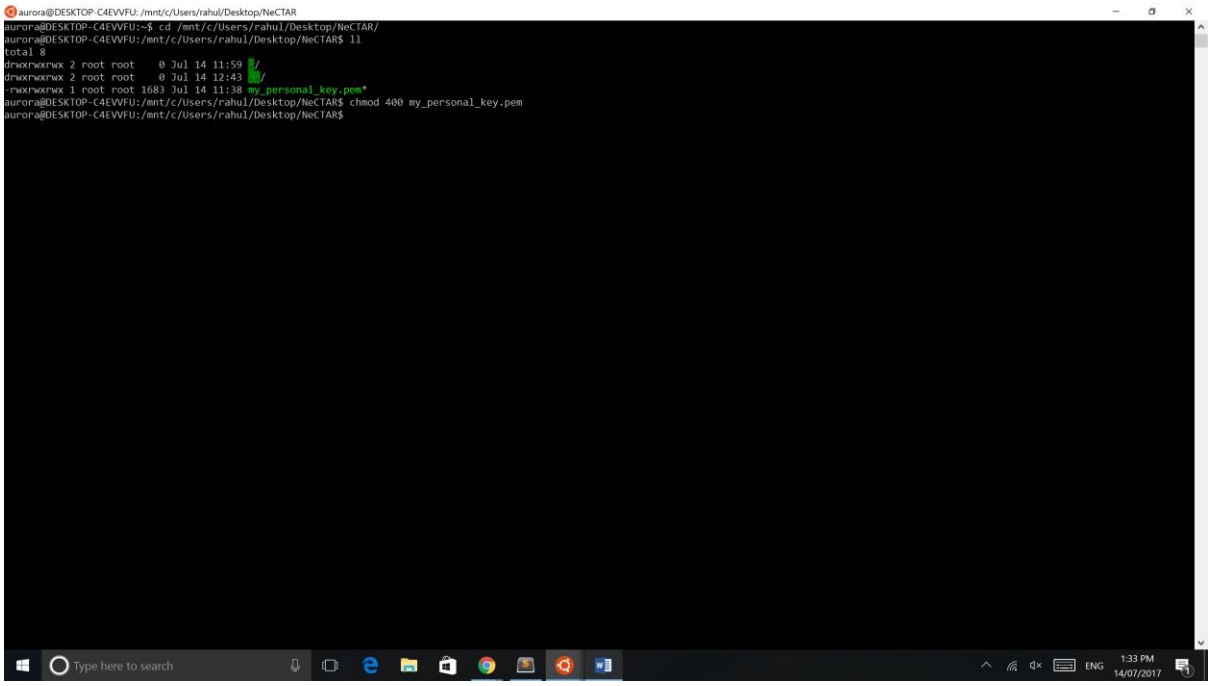
Open your terminal and direct yourself to the folder having the .pem keyfile that you just downloaded from NeCTAR. Use the ‘cd’ command to enter a particular folder. (Type “ls” <Representation in Caps: LS> in Mac to verify if your .pem file is there, I am using the Linux sub-system for Windows 10 so I can use “ll” <Representation in Caps: LL> instead).



Now type:

chmod 400 <name of your key>

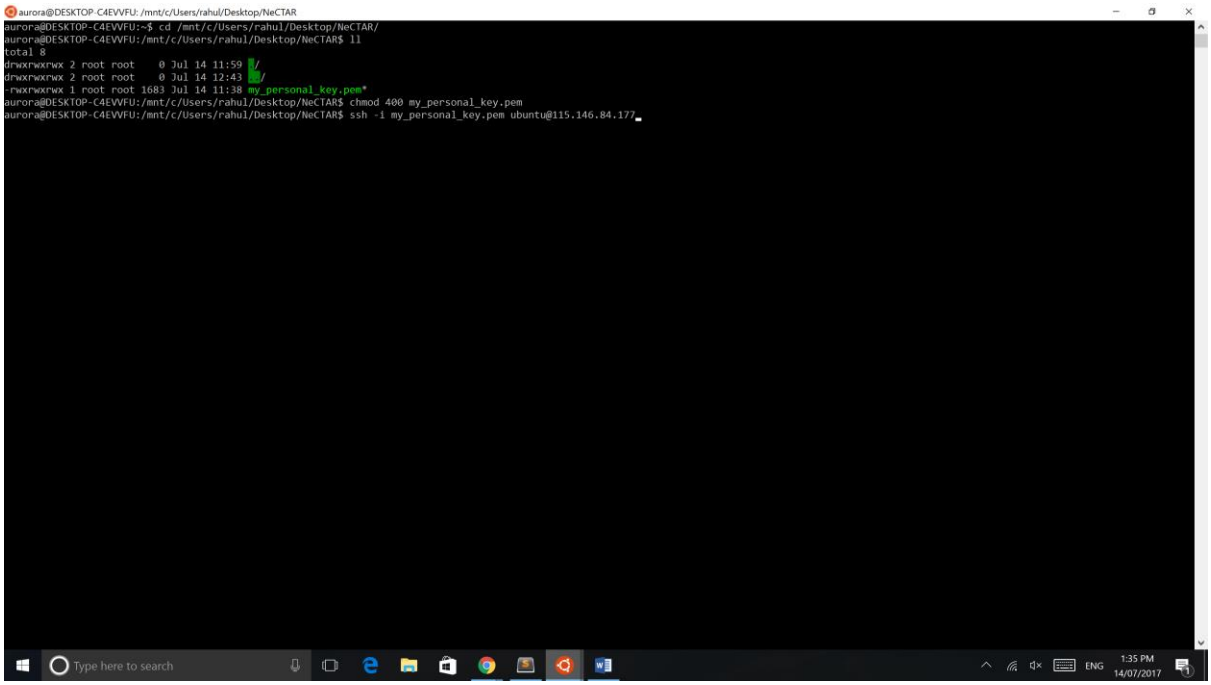
Now press enter. This will set the access rights to your key as only accessible via your profile thus making it more private (**this is required for using ssh**).



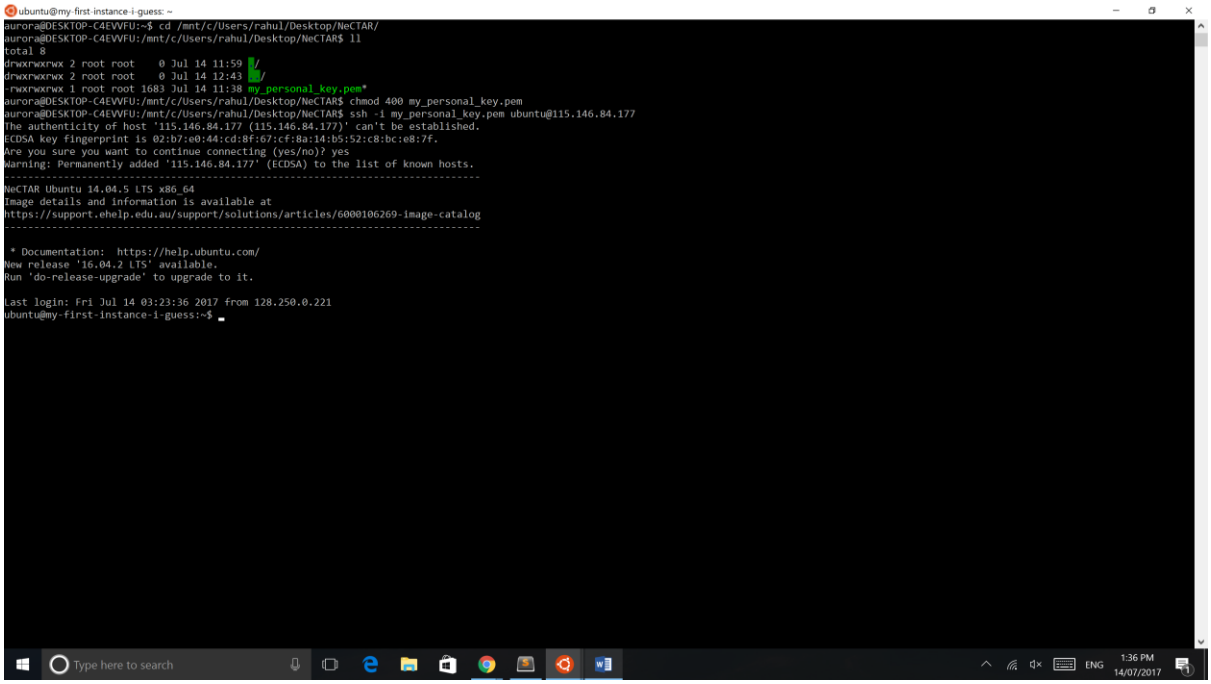
Now we need to type:

ssh -i <name of your key> ubuntu@<Ip address of your VM>

And press Enter.



You will get a message asking for whether you trust this signature and want to save it. Type: Yes and press Enter.



Congratulations! You managed to access your VM \(^.^)/.

WARNING:

1. Remember that NeCTAR is managed by a third party host and not you (nor us!!!!)… so please do things keeping in mind that someone else is monitoring each and every move you make (No privacy).

2. Going back to point 1, if you try to torrent files or host illegal content – you are liable to undergo legal proceedings. The academic staff will not help you if such a situation arises.

3. If your NeCTAR instance is no longer accessible then kindly contact NeCTAR support and not the teaching staff as we are not the system admins for this platform. If you are planning on running code on the cloud, do ensure that you have a local backup. Cloud is a volatile entity and any data stored on it is not guaranteed to remain as it is prone to faults (your instance crashes, the facility hosting the service gets affected, human related issues, etc.).

4. If you are going to request for more resources then please note that these allocations are not controlled by us so your request may be approved or rejected based on the application made and your reason for requesting the said resources. The teaching staff is not responsible for this.

5. Any and all urls present in this document are liable to change. If that does happen and the links in this document are useless then please use google. Google is love, Google is life ;).