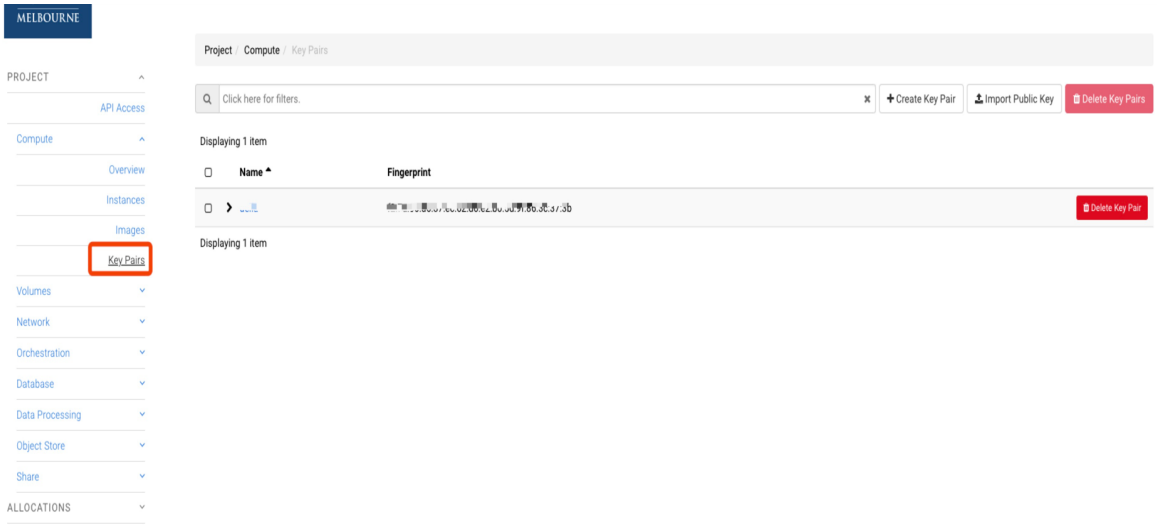
Virtual Machine Access in NeCTAR

1- When you create a new instance, you specify a key pair that will be used to connect to that instance securely. If you have used your own key pair, then you have a private key stored in your computer. Otherwise, if you asked NeCTAR to create a new key pair for you, you should have downloaded the private key, since without a proper private key you will not be able to remotely login to your instance.

2- If you need to create/import a new key pair or manage previously created key pairs, select the "Key Pairs" section of the dashboard as shown below.

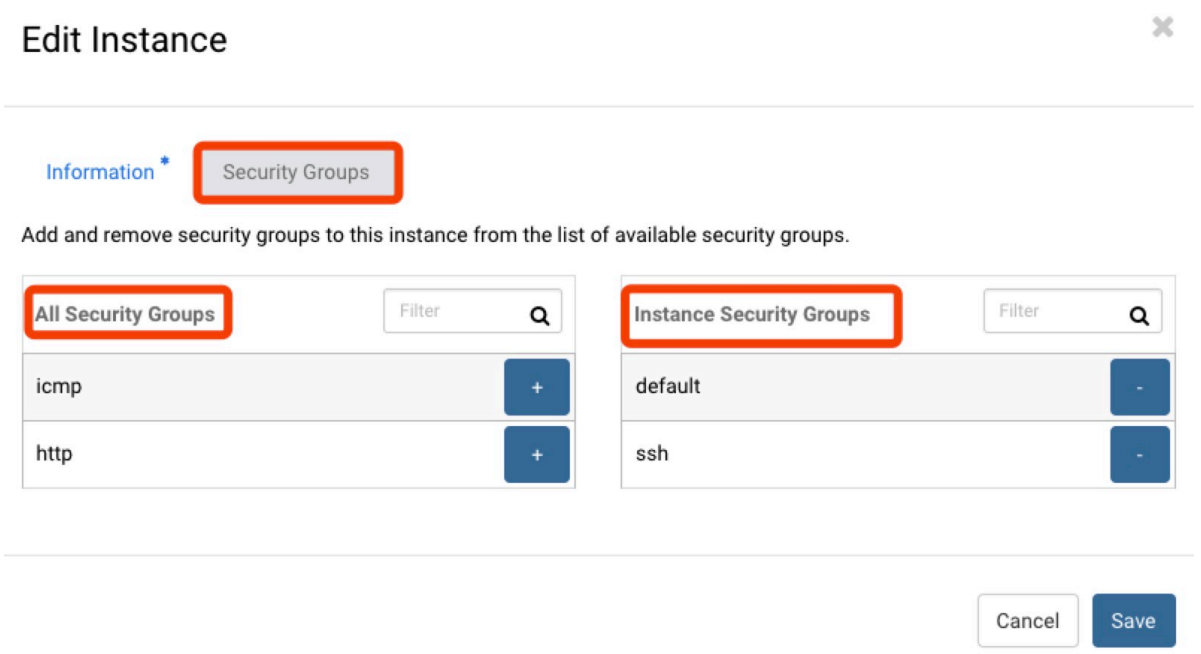


3- To access a specific instance, you need its IP address, the private key which will be used as a certificate for connecting to the instance, and an SSH client. The IP address can be found by logging into NeCTAR, choosing the appropriate project and selecting "Instances" from the left sidebar (for more information regarding this, refer to Using NeCTAR Dashboard tutorial). If you are using a Unix-based operating system such as

Mac OS or Linux, your system already has a built-in SSH client that can be accessed by opening a terminal. If using Windows, you need to download PuTTY and follow tutorials on the software's website about how to use SSH certificates for connecting to a remote instance. The rest of this tutorial assumes you are using a Unix-based operating system.

4- Locate your private key file and enter the following command in a local terminal (command prompt) to change the access permission of the key file: **chmod 600 <file name>**

5- Make sure SSH port (port 22) is open on the instance you want to connect. You can do so by selecting "Instances" from the left sidebar of NeCTAR dashboard and then clicking "Edit instance". Go to the "Security Groups" tab in the opened dialog box and there you can see which security groups have been added to that instance. Make sure "SSH" security group is added.



6- Open a local terminal window (command shell) and enter the following command to open an SSH session to the target instance: **ssh –i <path-to-private-key-file> ubuntu@<instance-ip>**

In the above command, ubuntu is the default username used for connecting to instances created from a Debian-based image. For connecting to instances that have been created from a CentOS or Fedora image, use **ec2-user** instead.