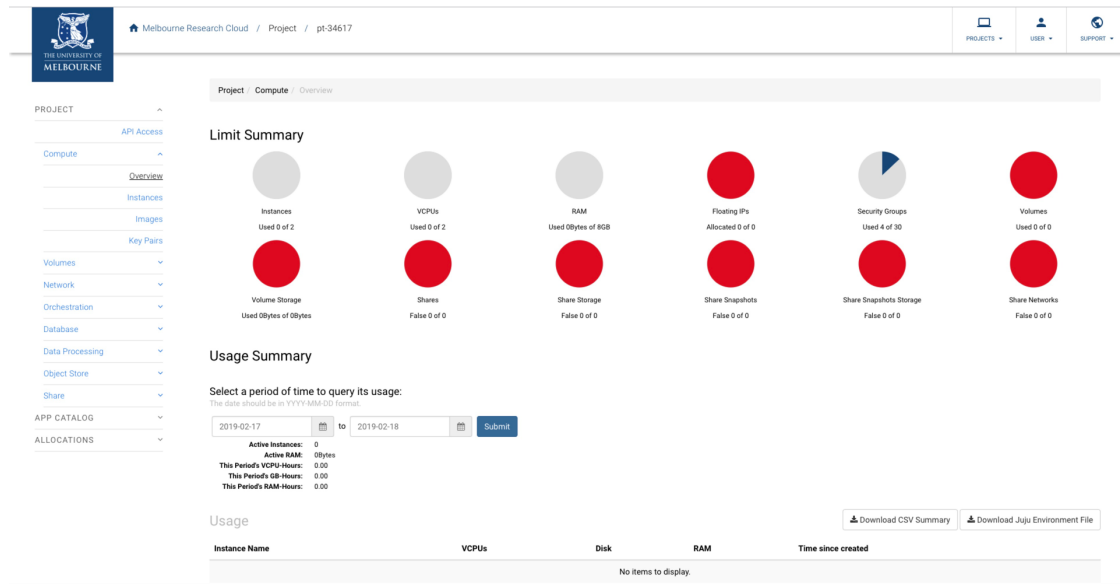
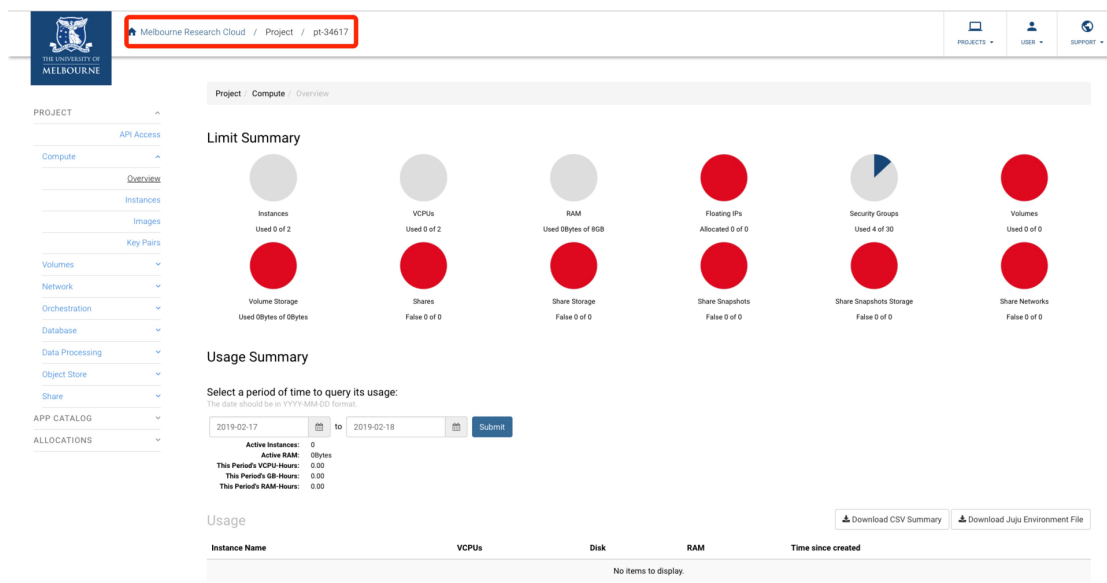


# Managing Security Groups in NeCTAR

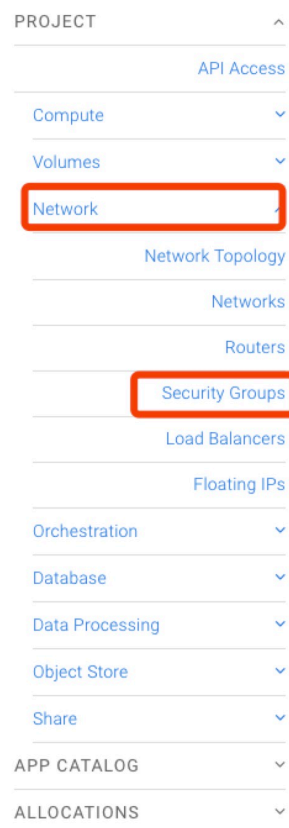
- 1- Login to the NeCTAR dashboard (refer to the tutorial demonstrating NeCTAR login procedure)



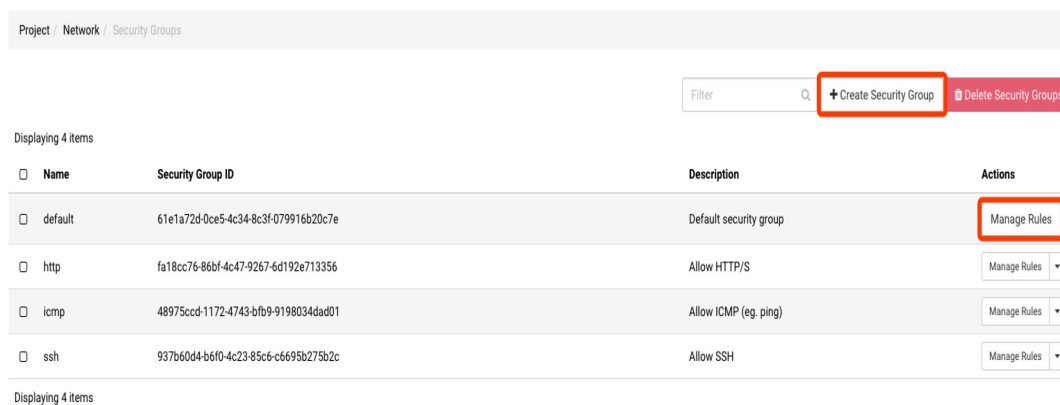
- 2- Select your desired project (note that virtual machines created in a project cannot be shared and seen in another project)



- 3- Select "Security Groups" under "Network" from the left sidebar.



- 4 All previously created groups will be listed. To create a new security group, simply click the “Create Security Group” button. You will be asked to provide a name and description for the new group.



- 5- Each security group contains rules that define which ports and corresponding protocols should be allowed and what should be restricted. To modify the rules within any security group, click the “Manage Rules” button in front of its name.
- 6- To create a new rule, click the “Add Rule” button. In the new rule dialogue box, first choose the rule type that identifies the protocol being used. Options include selecting custom TCP or UDP rule for a specific port or using predefined templates such as SSH or HTTP that will open ports 22 and 80 respectively. Then enter the port number or port ranges in their appropriate section. Final step is entering the IP address range that should be able to access resources on that instance. This should be achieved using CIDR notation that is beyond the scope of this tutorial.

✕

### Add Rule

---

**Rule \***

Custom TCP Rule 1

**Direction**

Ingress

**Open Port \***

Port 2

**Port ?**

3

**Remote \* ?**

CIDR

**CIDR ?**

0.0.0.0/0 4

**Ether Type**

IPv4

**Description:**

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

**Rule:** You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

**Open Port/Port Range:** For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

**Remote:** You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel

Add

- 7- To see which security groups are active on a particular instance and add/remove them, select “Instances” from the left sidebar of NeCTAR dashboard and then click “Edit instance” on the right. 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.

## Edit Instance



Information \*

Security Groups

Add and remove security groups to this instance from the list of available security groups.

All Security Groups	Filter	Q
icmp		+
http		+

Instance Security Groups	Filter	Q
default		-
ssh		-

Cancel

Save