OpenStack [Beta] MS-Windows VM User Manual

Version: V_0.1

04 April 2022

Version Control

Version	Date	Amended by	Summary of Changes
0.1	04 April 2022	Liu Yuancheng	Init the doc draft.

Contents

1. Introduction

Doc description:

This manual will be used by National Cybersecurity R&D Lab (NCL) customers as a reference for creating a Microsoft Windows VM in their project under NCL OpenStack [Beta] Testbed and use the RDP (remote desktop client) to remotely access their Windows VM in their instance from local computer. The document contains 2 main sections, the **Windows VM Creation** section will introduce the detailed steps to create the VM under an instance. The **VM Remote Access** part will introduce how to config remote access to VM from user's local computer.

Doc Type: External User [Customer] Manual, All NCL external users.

2. Windows VM Creation

Follow the steps 2.1 to 2.3 below to create a Windows VM in an instance under user's project.
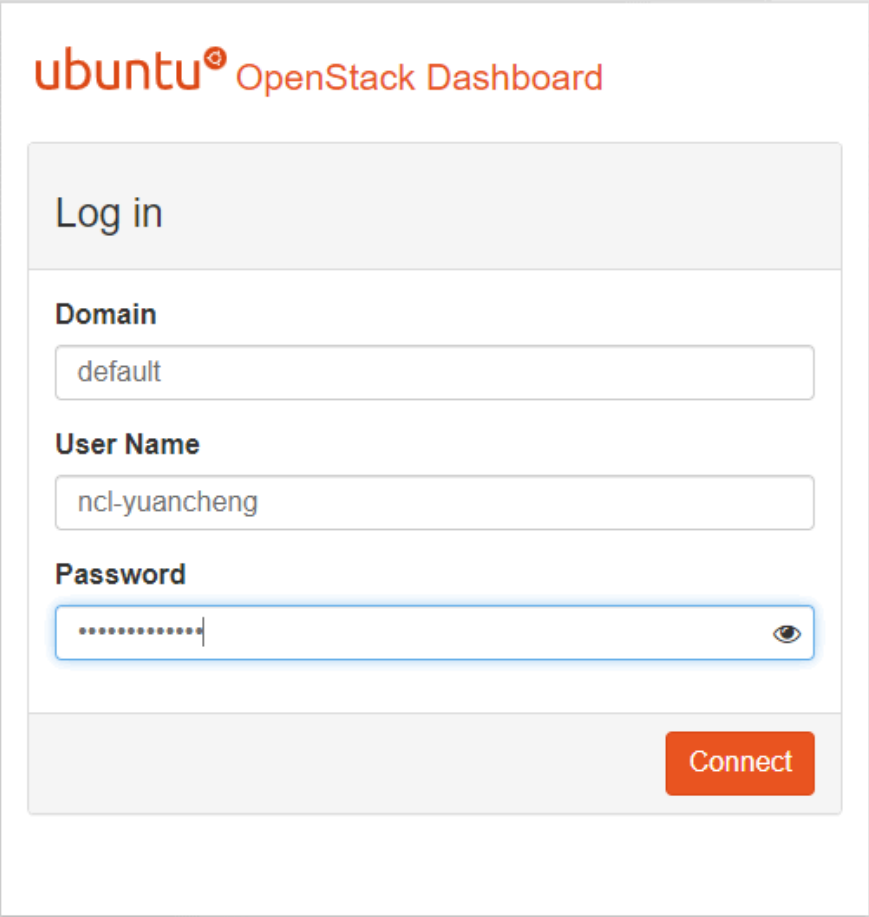
2.1 Login the NCL OpenStack Platform

OpenStack [Beta] platform link: https://openstack.ncl.sg/

Login with the ncl-openstack account and password under domain **default**. (As shown below)

Domain: default

Username/password: <customer ncl username>/< customer password >

NOTE: If there is any login problem or you don't have an account on the NCL OpenStack platform yet, please contact NCL Support (support@ncl.sg).

2.2 Create an Instance with Windows-VM-Image

Follow below steps 2.2.1 to 2.2.3 to create an instance with a NCL public Windows-VM image. In this section, we use MS-Windows 10 Professional x64 as an example.

2.2.1 Access the Instance Creation Page

After user login OpenStack [Beta] platform web (as shown below), please select your project and access the instance creation page and follow the below steps:

Step_1: Select your project in the top drop-down menu. If you don't have a project yet, please create a new project or contact NCL-support (support@ncl.sg).

Step_2: In the left side navigation panel, select Project => Compute => Instances to instance management page.

Step_3: In the instance management page select launch Instance button.
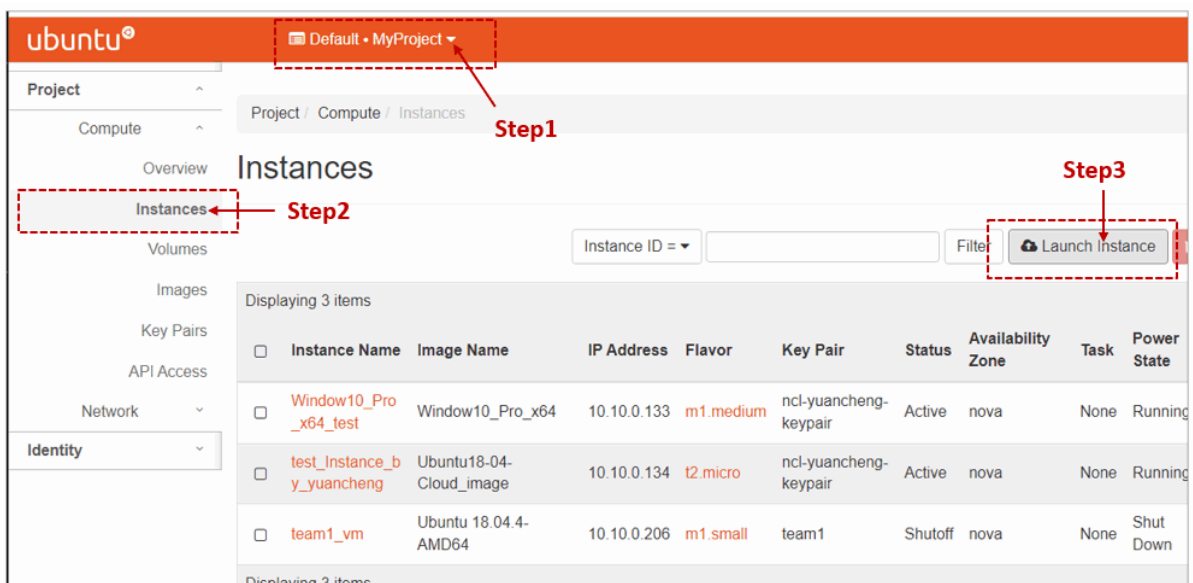
2.2.2 Create an Instance with Windows-VM Image

After the instance configuration dialog pop-up, config the instance with below steps:

Step_1: Add a unique instance name (instance ID) in the "Details" config page (as shown below).

Use default setting:

- Availability Zone: **nova**.
- Instance Count: **1**;

Step_2: Click "Next" then switch to `**source**` page to select the Image, in the public VM-image (*qcow2) available list select the Windows VM image you want to use (Windows10_Pro_x64) and press the '**up**' arrow button to add the image to the allocated list.

Use default setting. Select Boot Source: `**image**` ; Create New Volume: `**No**`;

Note: Public image can be used in any instance, but private image can only be used in your own project instance.

Step_3: Switch to "Flavor" page to select the image instance hardware config. Press the 'up' arrow button to add the flavor as shown below (We prefer use to use the `m1.medium` or higher level flavor for all the Windows VM):
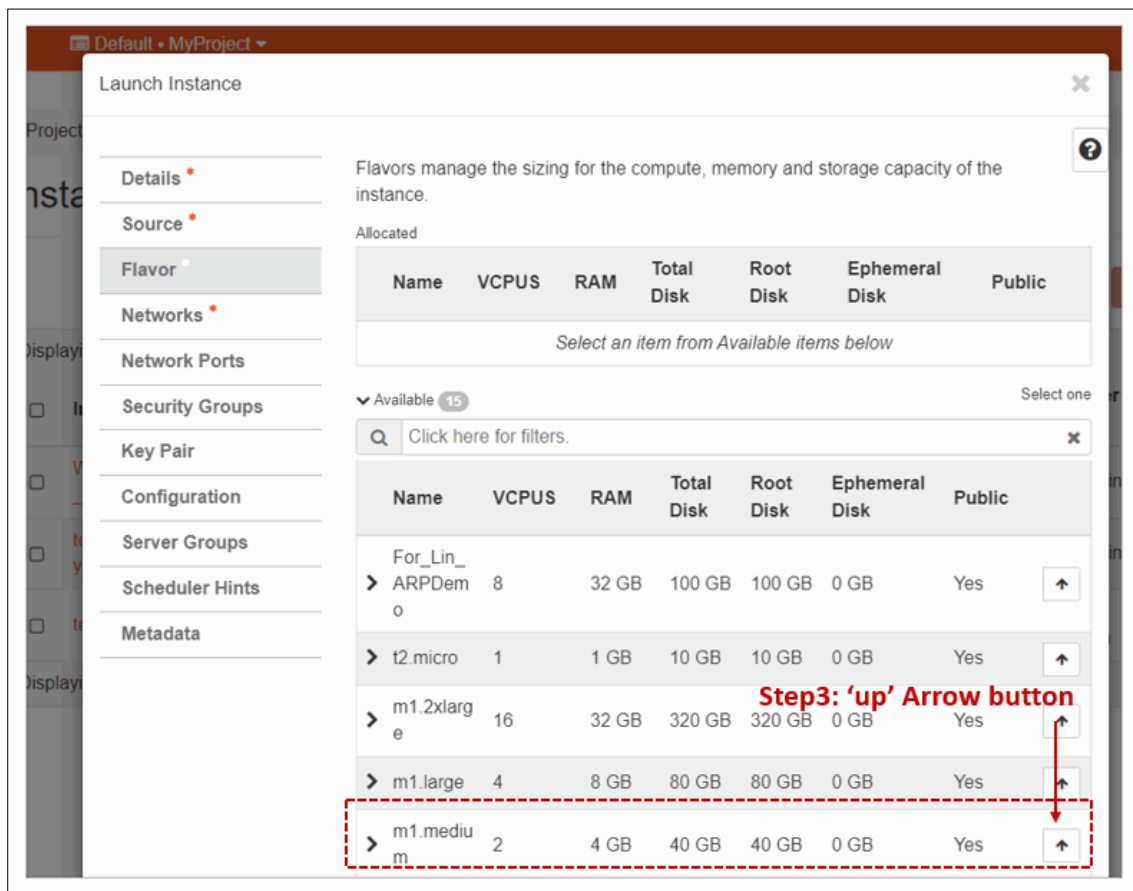

Note: If the flavor shows "alert" icon of the flavor (as shown below), that means your instance doesn't have enough capacity for allocating the hardware flavor. Choose a flavor which does not contain any "alert" icons. Otherwise, please contact NCL support team to extend the instance capacity if you wish: support@ncl.sg .
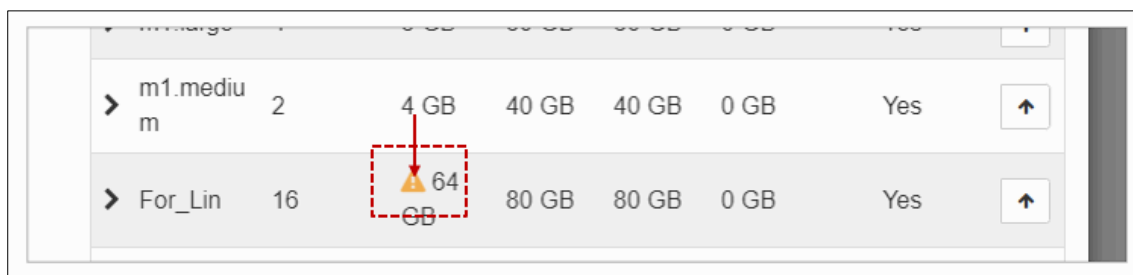

Step_4: Switch to "**Networks**" config page and select provider config. Press the 'up' arrow button to add the provider network (as shown below).

Note: If you want to login to your instance using SSH, you must add the instance to the provider network or assign a floating IP address (e.g., 10.10.0.111) to the instance. In addition, make sure that the 'default' security group allows ICMP (ping) and secure shell (SSH with TCP port 22).
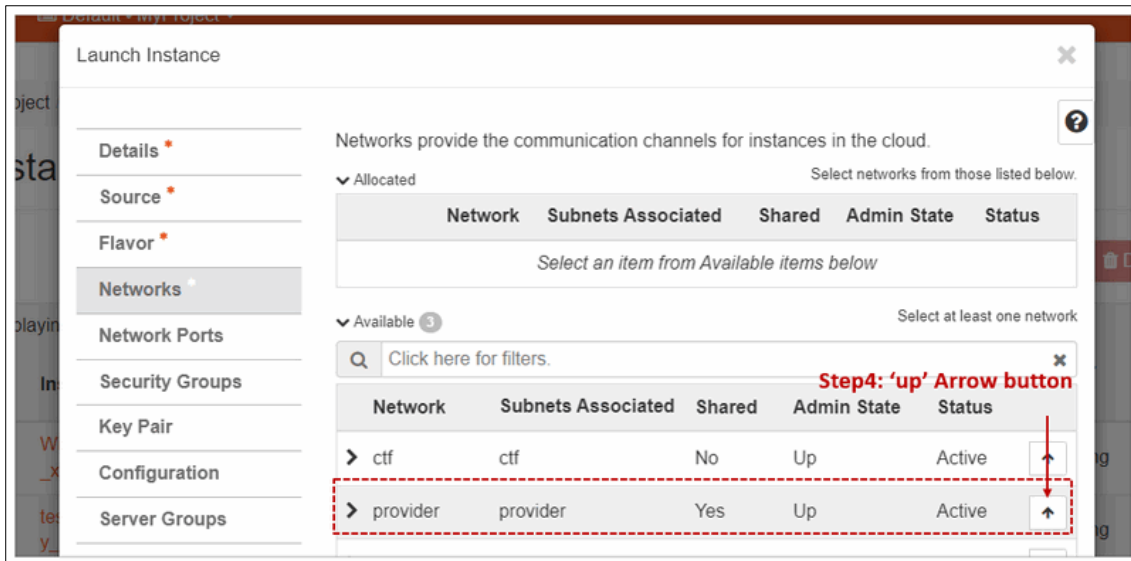
Step_5: Switch to "Key Pair" page to create the keypair. Press the `**Create Key Pair**` button. Type in the keypair name and download the keypair `**\*.pem**` file and keep it in your own device.
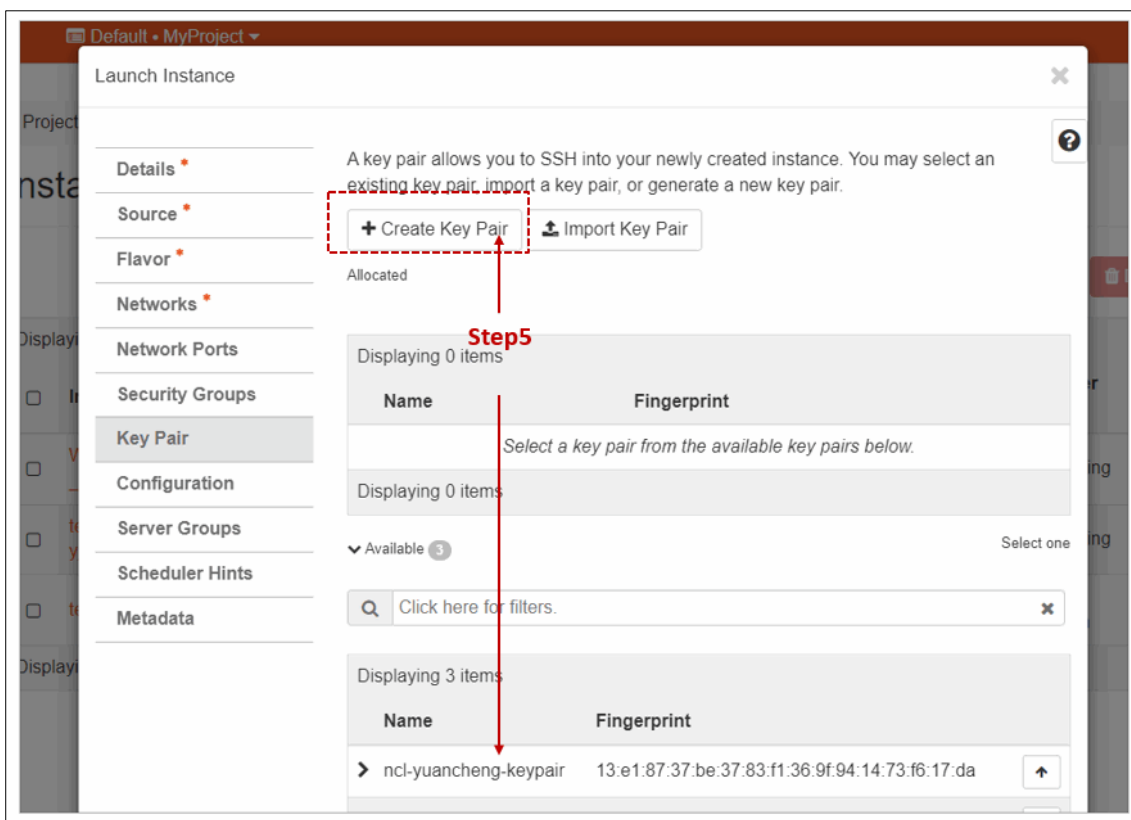

Note: If you have your own *.pem file, you can select the import key pair. You may also use the key pair you created before. The key pair you created will be shown in the available list.
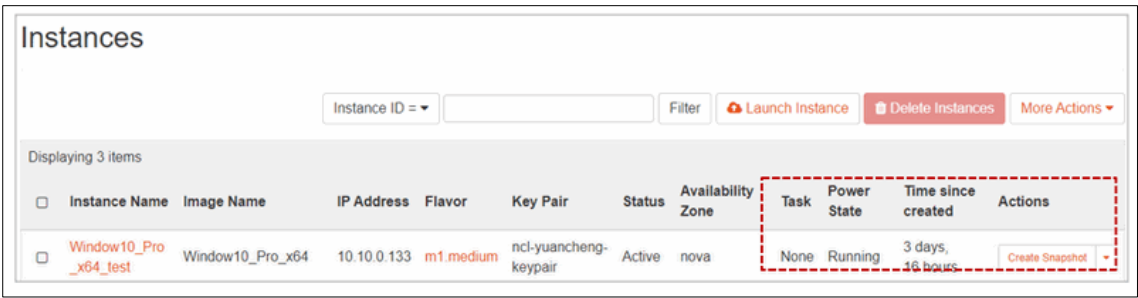
Step_6: Finish all the other setting pages with the default setting, and press the "Launch Instance" button to launch the VM. (As shown below)
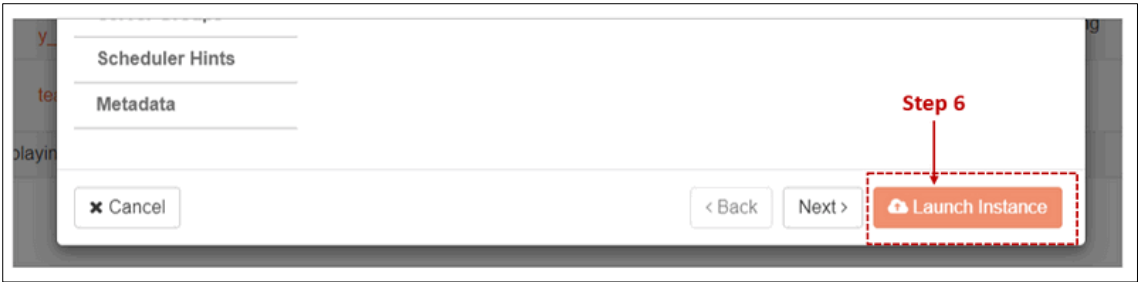
After the instance launched, you can see the instance is under spawning:
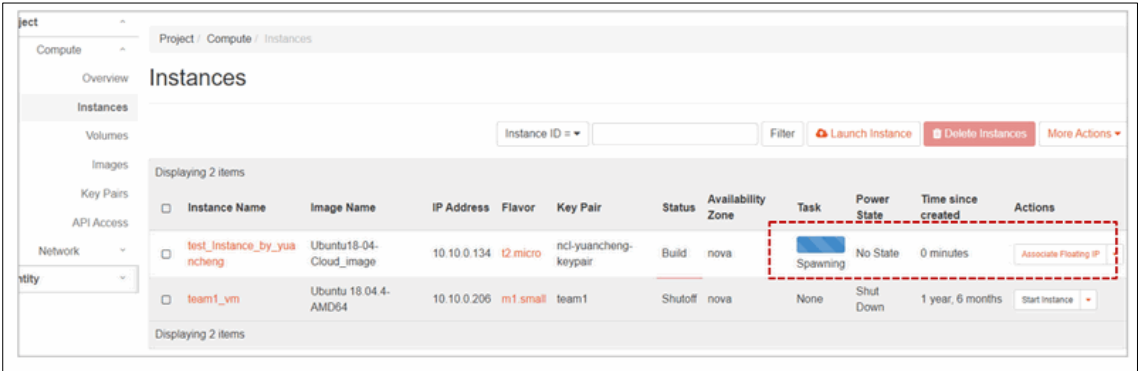
When the "Power State" shows Running, the instance is ready for using:

## 2.3 Config the Windows VM Security Access [Optional]

The security and most networking settings will be done by NCL staff. External user/customer may just configure internal network among multiple VMs in his/her project.

2.3.1 Config the Instance Network Security Group [Optional]

Step_1: Select "**Edit security group**" in the instance actions drop down menu:
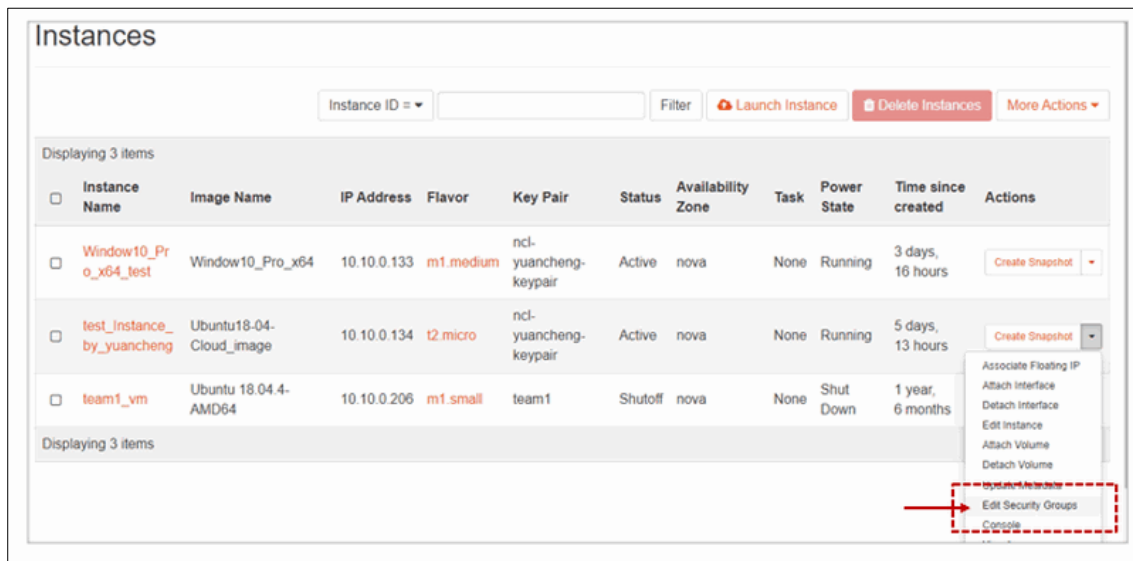
Step_2: Select the security group you want to add to the instance as shown below (we prefer the default_no_internet):
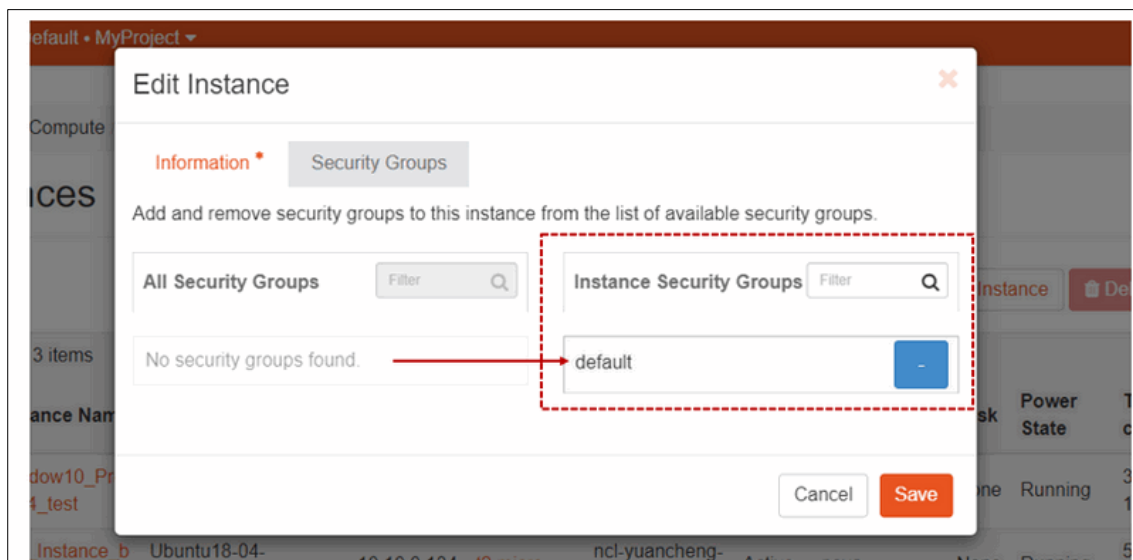
Note: We prefer user use the security group configed below:

- **Default** [internet, SSH, RDP];
- **Default_no_internet** [RDP, SSH];

Default network police rules:

	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group
				Displaying 6 items		
☐	Ingress	IPv6	Any	Any	-	default
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-
☐	Egress	IPv6	Any	Any	::/0	-
☐	Ingress	IPv4	Any	Any	-	default
☐	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-
☐	Ingress	IPv4	TCP	3389 (RDP)	0.0.0.0/0	-

Displaying 6 items

Default_no_internet network police rules:

Displaying 4 items

	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix
☐	Egress	IPv4	ICMP	Any	0.0.0.0/0
☐	Ingress	IPv4	ICMP	Any	0.0.0.0/0
☐	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0
☐	Ingress	IPv4	TCP	3389 (RDP)	0.0.0.0/0

2.3.2 Check the Windows-VM running [Optional]

Select the instance webpage (click the instance name) and press the console tab to access the VM directly [**username**: ncl_win64_pro, **password** 123] :

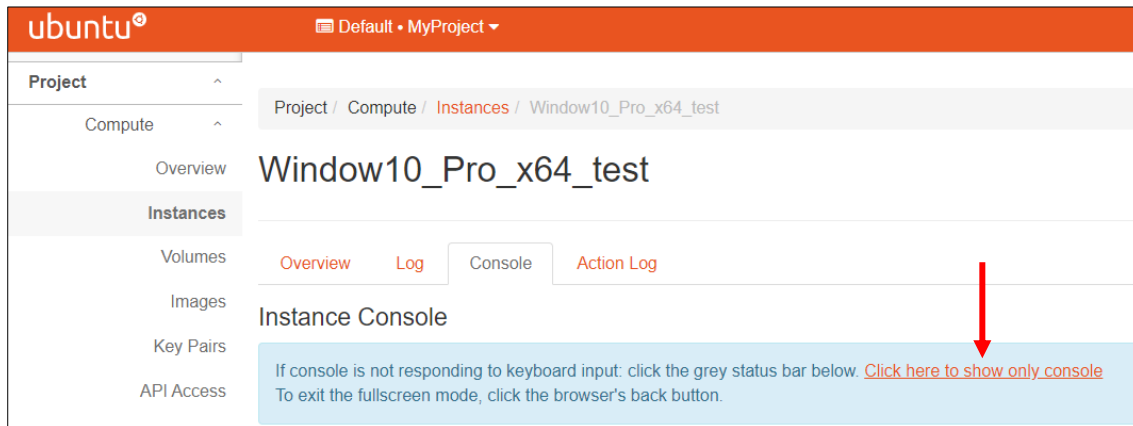Then the webpage will show the VM desktop, please switch to full screen by click the button "**Click here to show only console**" in "**console**" tab so you can type in the password **123**.
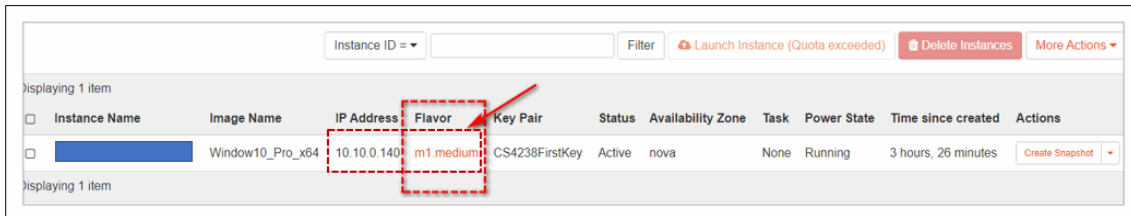

Confirm the remote desktop has been enabled:
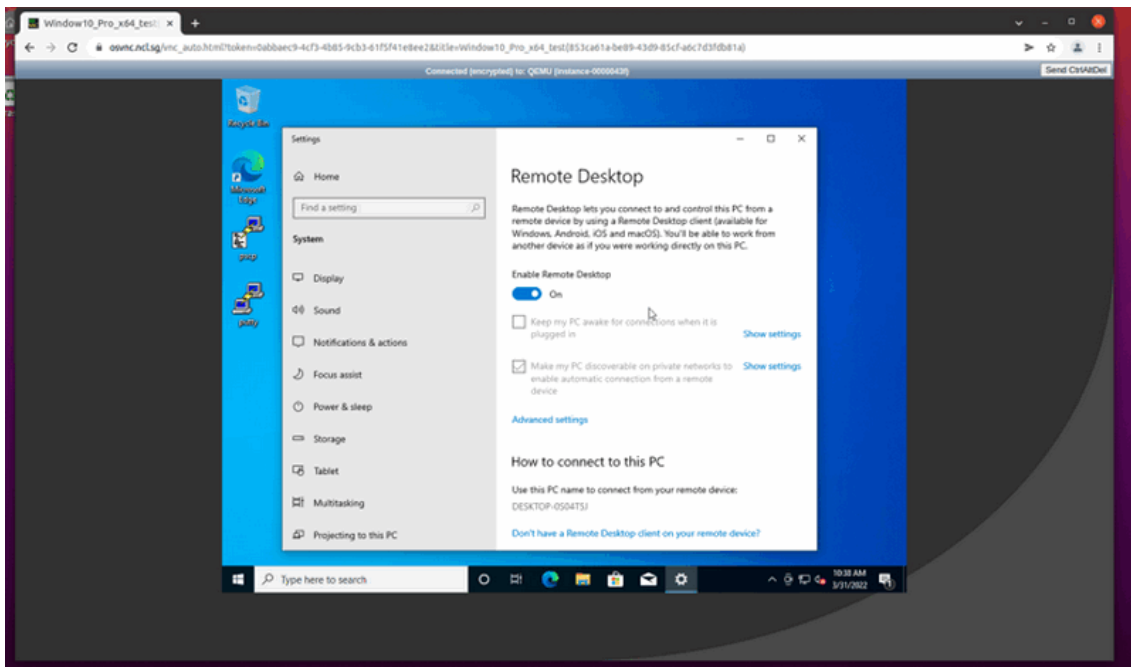
Note: We recommend customer to change the default password **123** to their own password.

3. Remote Access the Windows VM

Follow below steps to remotely access the Windows VM from user's local computer using RDP software. Get the instance internal IP address from the instance list (as shown below the IP address is **10.10.0.140**):


Step_1: login the NCL gateway (SSH to gateway.ncl.sg) with your gateway account and do the port forwarding: open a cmd terminal on your local machine and run the cmd:
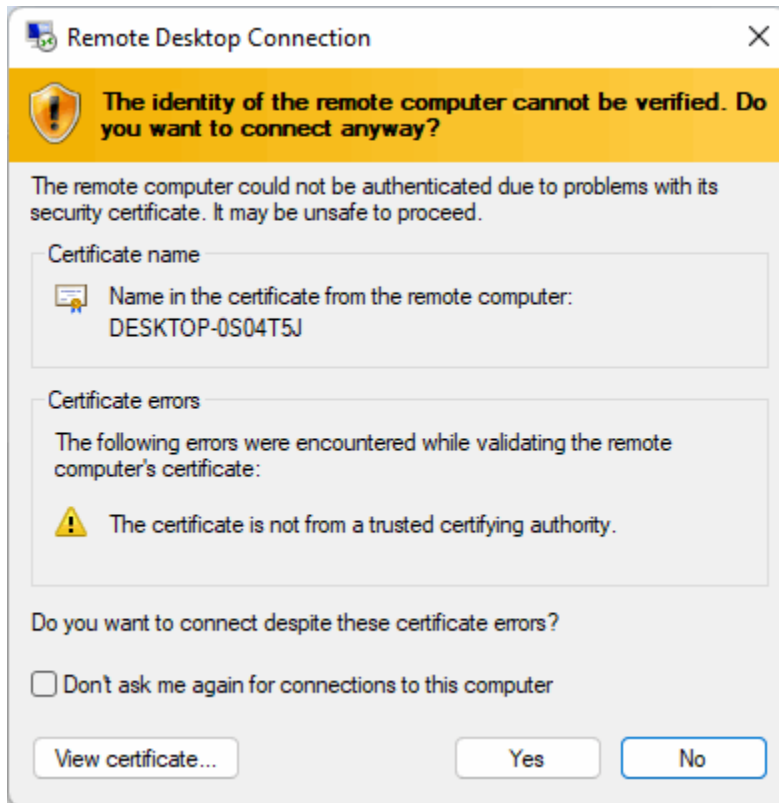
```
ssh -L 3389:<instance ip address>:3389 <username>@gateway.ncl.sg

example: ssh -L 3389:10.10.0.140:3389 ncl-yuancheng@gateway.ncl.sg
```

Step_2: Open Windows RDP client and fill in the IP address **127.0.0.1,** username: **ncl_win10_pro.**
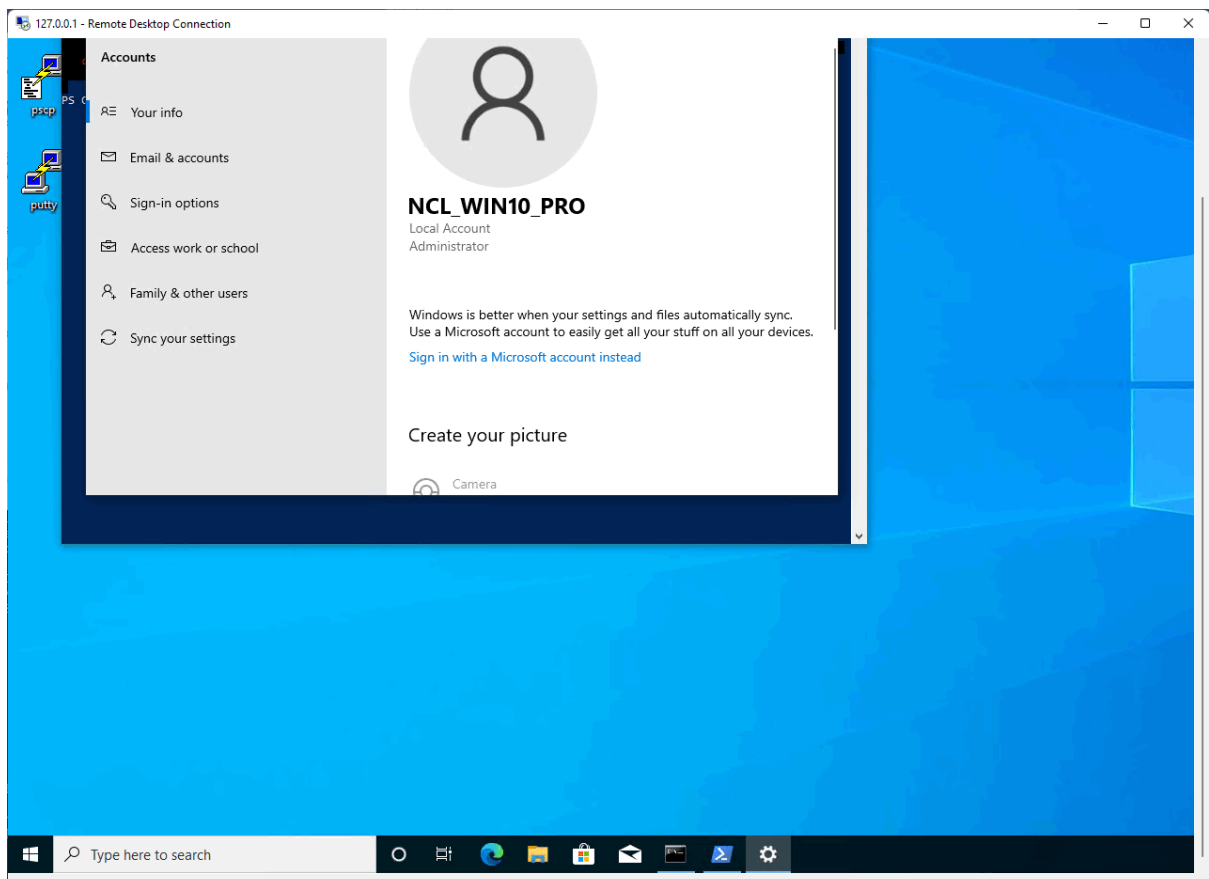
Step_3: Click the "Connect "button and when the password input dialog popup, type in password **123.**
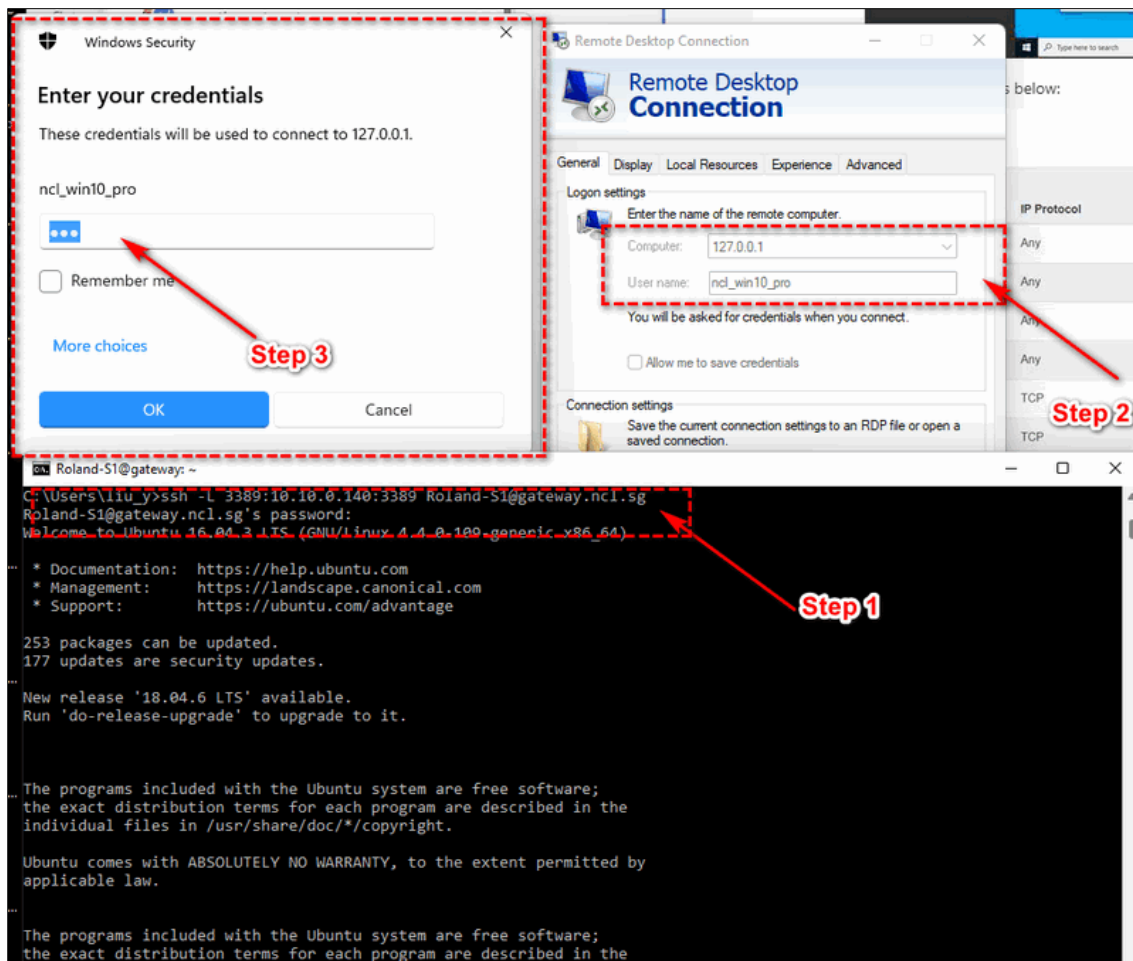
Press "**Yes**" when the connection certification alert window pop-up:

Then You can use RDP to access the VM as shown below:

4.File Transfer [Optional]

If the users want to transfer files from their local computer to the OpenStack VM or download files from the OpenStack VM to their local computer, they can follow below steps:

Step 1: Click "**Show Options**" within the RDP window (the RDC configuration options).
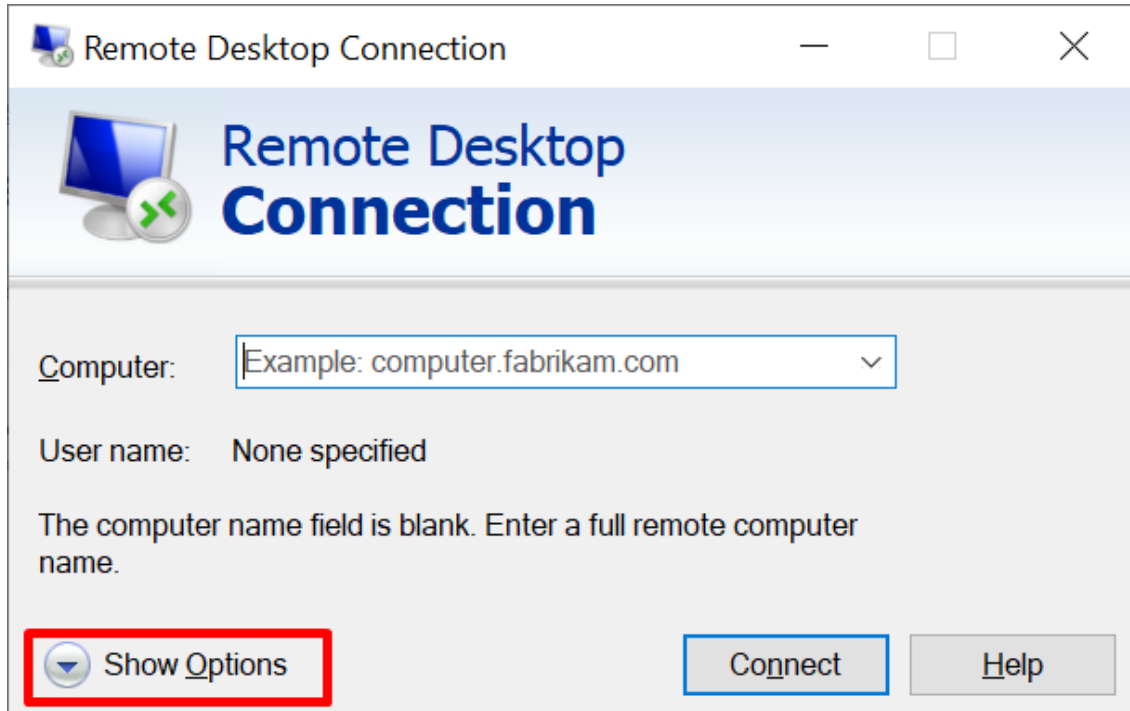
Step 2: Click "**Local Resources**" tab then select "**More**", after that check the volume you want to config as a network shared driver.(as shown below, the local driver E: is configured as shared driver)
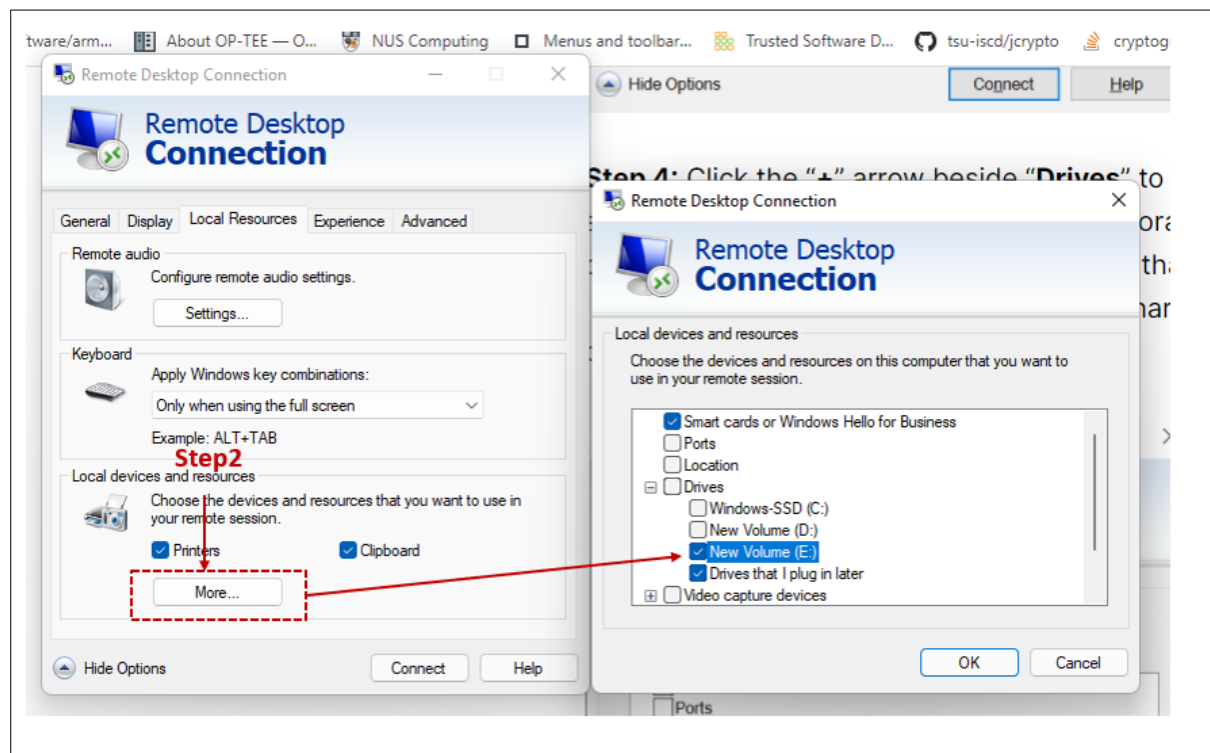
Step 3: In RDP window, the user needs to click the **network** => **tsclient** => **\\tslient:E** , then he can see the shared network driver and he can drag file in to the VM or download the VM file to his local computer. (As shown below)
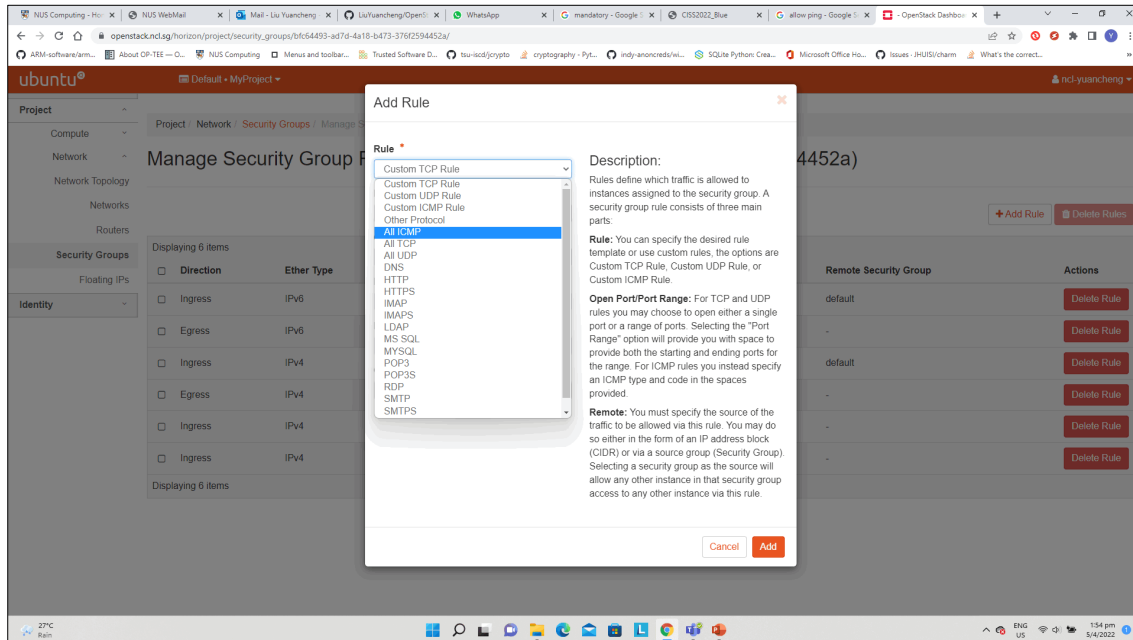

Reference: https://www.helpwire.app/blog/remote-desktop-transfer-files/
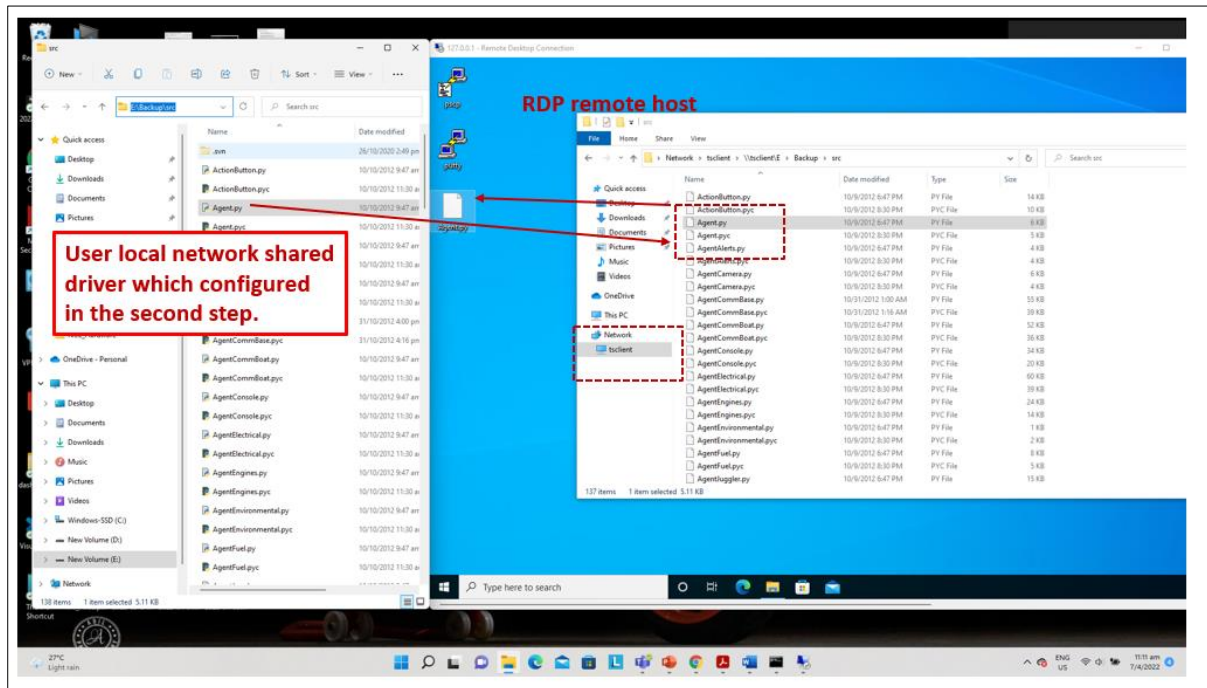
Appendix

Enable ping Windows VM from another server:

1.Enable the ICMP network policy rule:

2. Enable the ICMP in Windows VM firewall: