# How to create Hadoop on your Metacentrum account

## Content

# Quick guide

1. Fill an application here: https://metavo.metacentrum.cz/osobniv3/wayf/proxy.jsp?locale=cs&target=https%3A%2F%2Fsignup.e-infra.cz%2Ffed%2Fregistrar%2F%3Fvo%3Dmeta%26locale%3Dcs
2. Enter the information that you belongs to CVUT:FEL:B0M33BDT, ev. CVUT:FEL:A4M33BDT
3. When it will be approved visit: https://cloud.metacentrum.cz/
4. Click on Dashboard, log in as EINFRA CESNET
5. Follow the instructions here: https://wiki.metacentrum.cz/wiki/Hadoop#OpenStack_CLI_-_jednostrojov%C3%BD
    a. 2.2OpenStack GUI (Horizon) – jednostrojový

# Manual

## Prerequisites

It is **highly recommended** to generate your SSH keys pairs before creating a new instance. You can do it using Command Line or application PuTTY. Otherwise, you may also generate SSH keys when creating a new instance (see further manual).

## Generate SSH via Command Line (recommended)

**Note:** this manual is written for Windows command line. If you use linux, just change all paths to standard linux paths (**/home/<your_username>/.ssh/<ssh_keys_name>**)

1. Open command line and put command **ssh-keygen** (Fig. 1).


Fig. 1 - ssh-keygen Command Line Interface example

2. You will be asked where to save the generated public and private keys. Save it to the **.ssh** directory **C:\Users\<your_username>\.ssh\<ssh_keys_name>** (Fig. 2).
   a. If you don't see **.ssh** directory, try to enable showing hidden files and directories.
   b. If you still don't see **.ssh** directory, create it.

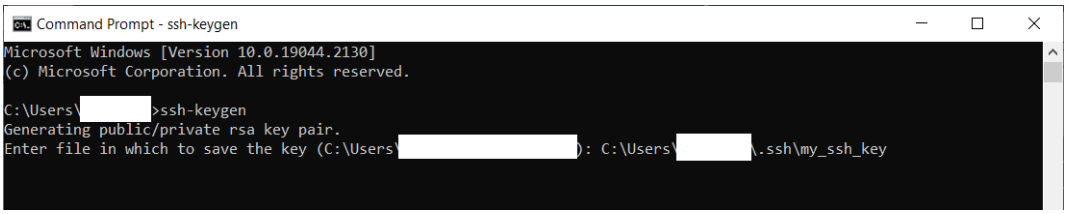


Fig. 2 – ssh-keygen Command Line Interface. Path to save SSH keys

3. Then you will be asked to enter a **passphrase**, which is a password you will be asked to enter every time you use your SSH key. Using passphrases is recommended in terms of security, but entering passphrase **is optional**, so you can skip it by pressing "Enter" (Fig. 3).

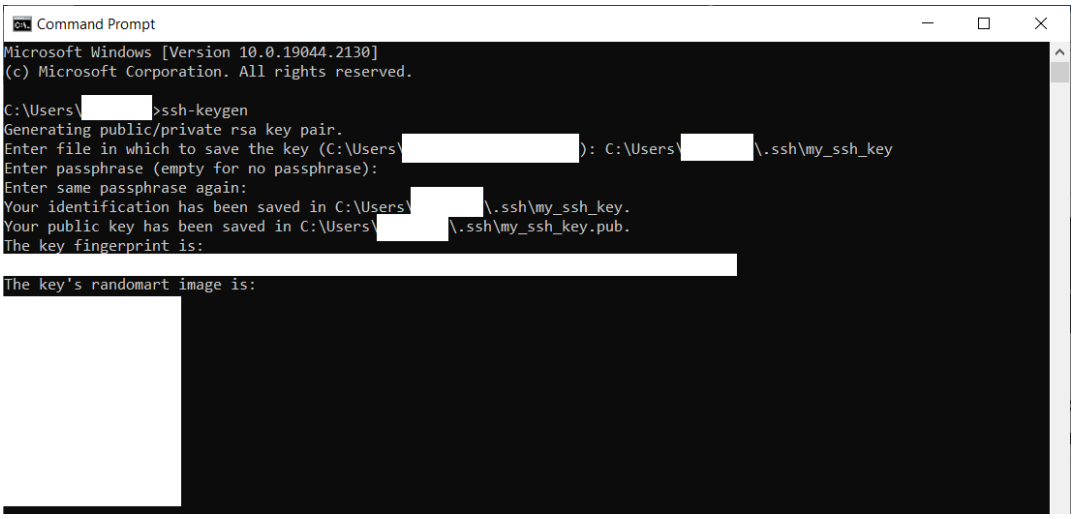


Fig. 3 - ssh-keygen Command Line Interface. Path to save SSH keys

4. Check that your keys are in the directory **C:\Users\<your_username>\.ssh**
5. **Don't lose it ☺**

## Generate SSH via PuTTY

1. Open PuTTY Key Generator (PuTTYgen) (Fig.4)

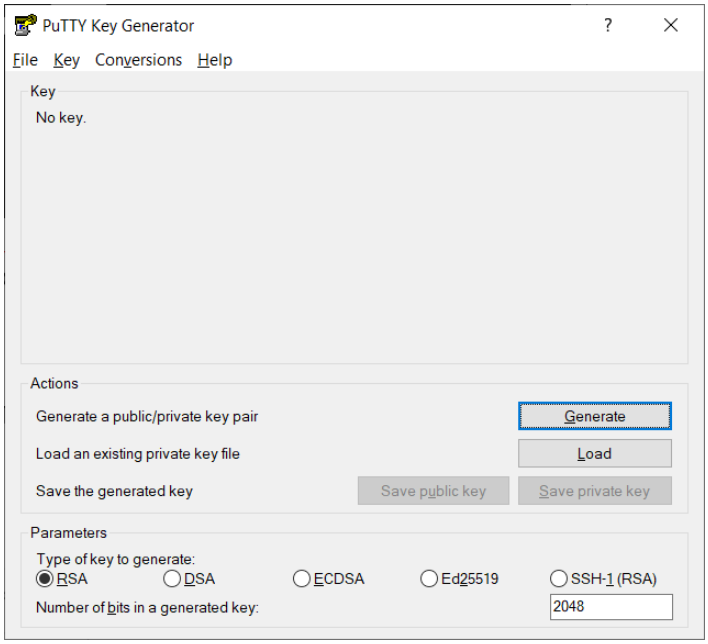


Fig. 4 – PuTTYgen application

2. Click "Generate" button and randomly move your mouse over the blank area (Fig. 5)

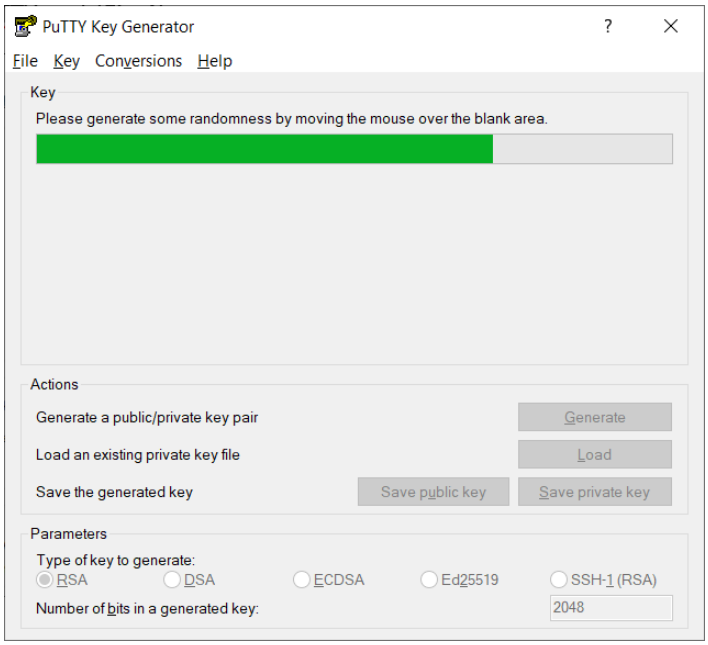


Fig. 5 – Generating SSH keys via PuTTYgen

3. Once your keys are generated you may enter a **passphrase**, which is a password you will be asked to enter every time you use your SSH key. Using passphrases is recommended in terms of security, but entering passphrase **is optional** (Fig. 6).

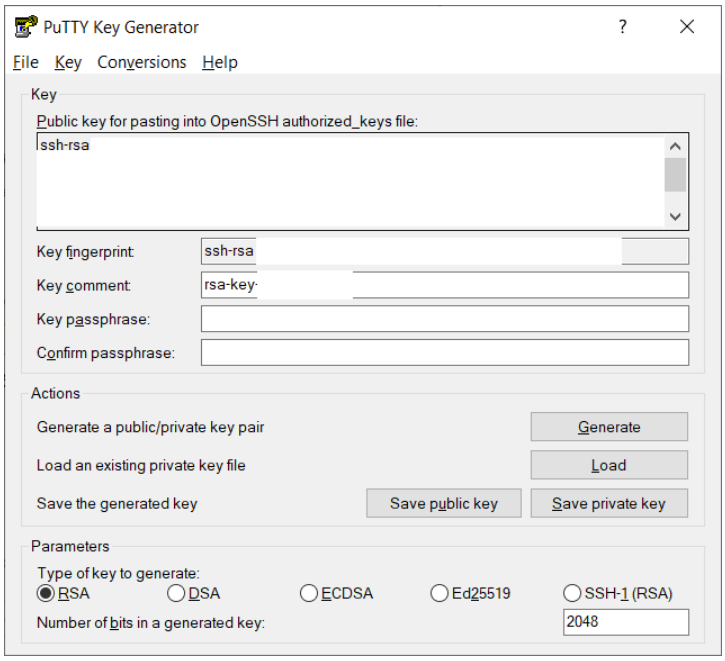


Fig. 6 – Generated SSH keys via PuTTYgen

4. Save your public and private keys in the directory **C:\Users\<your_username>\.ssh** using buttons “Save public key” and “Save private key” respectively.
5. Check that your keys are in the directory **C:\Users\<your_username>\.ssh**
6. **Don’t lose it** ☺

# Instance creation

1. On the left menu click on “Compute”
    - Click on the Images screen
    - Find the image: `debian-9-x86_64_hadoop`
    - Click on “Launch”
2. Fill the instance name (Fig. 7), click on “Next”

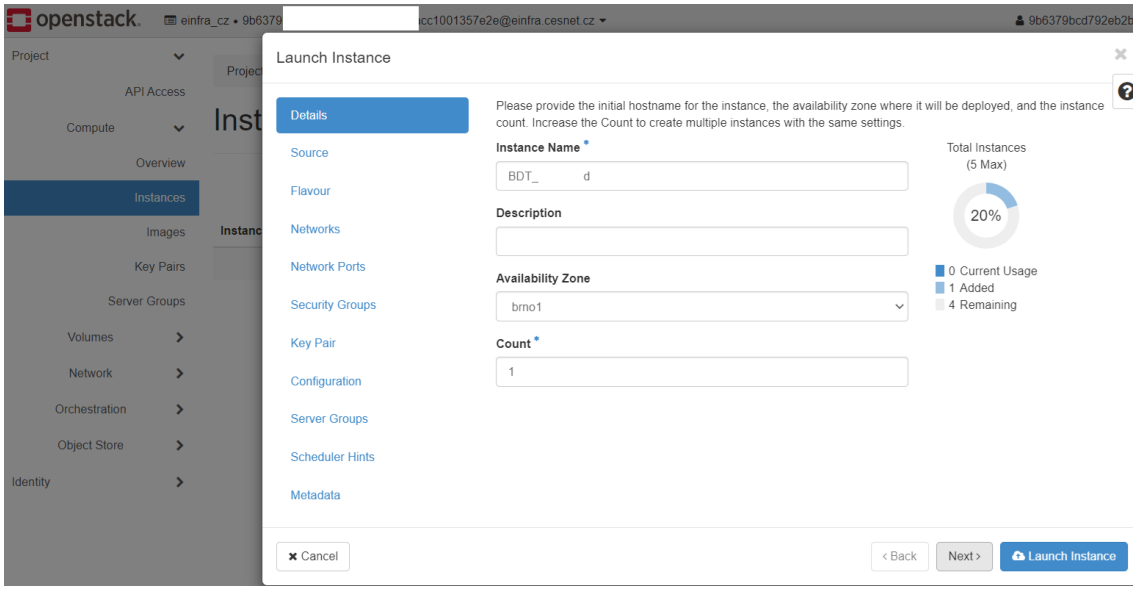


Fig. 7 – Instance details

3. Increase the disk **volume size** to 40-80 GB, check the image once more. Click on “Next”.

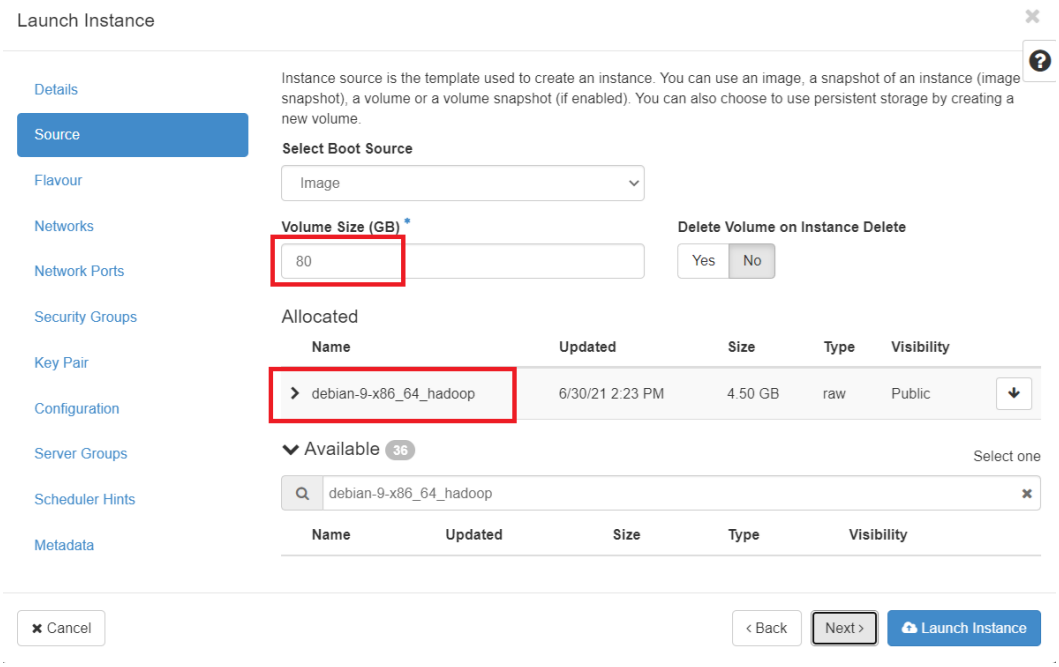


Fig. 8 – Source settings

4. Choose **medium** or **large** instance (Fig. 9). Click on “Next”

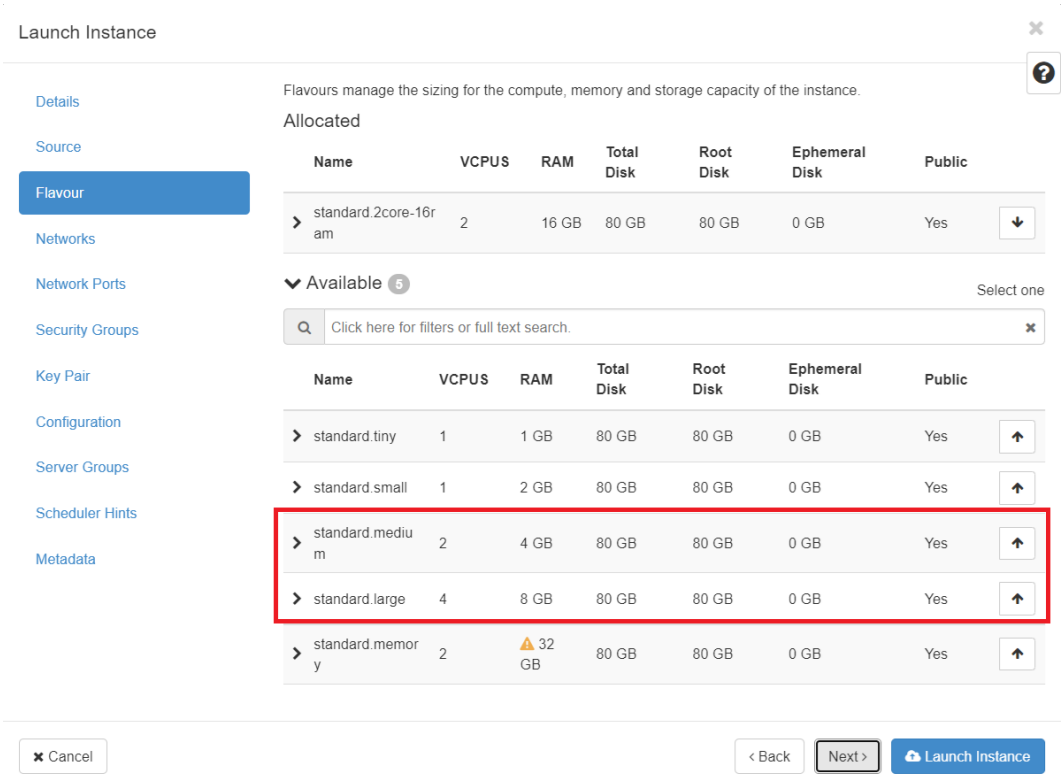


Fig. 9 – Flavour settings

5. **(IMPORTANT!!!) Choose the “147-…” network (as it is shown in the Fig. 10 in section “Available” in the red rectangle),** otherwise you will not be able to reach your machine! *(**Note:** If you have any other network selected in “Allocated” section like in the Fig. 10: network “78-128-250-pers-proj-net”. **It is WRONG! Remove it and allocate “147-…” network instead**).*

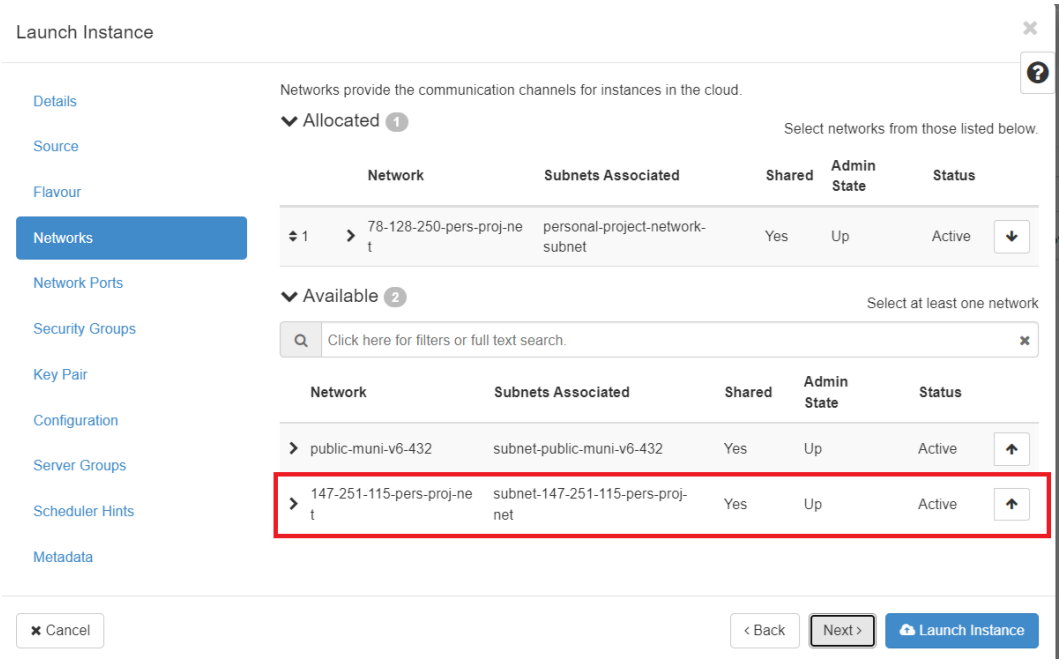


Fig. 10 – Networks settings

6. **(IMPORTANT!!!)** On the left menu click on “Key Pairs”.
   **If you have created SSH keys** as it was described at the beginning of this manual in the “Prerequisites” section, just import the **PUBLIC** key (***Attention: NEVER import/upload your private SSH key!!!***) by pressing “Import Key Pair” button (Fig. 11).

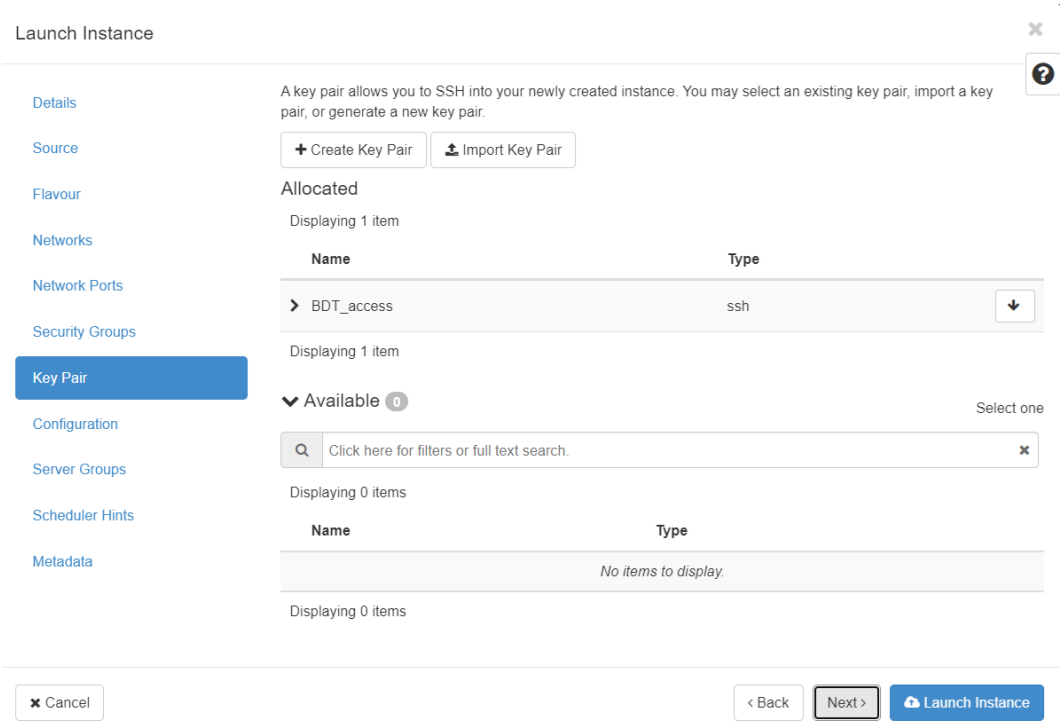


Fig. 11 – SSH Key Pairs settings

In the appeared form:

- Fill the “Name” field
- In the field “Type” select “SSH”
- Import the **PUBLIC** SSH key
- In the field, where your **PUBLIC** key is appeared, scroll down and remove last empty row
- Confirm

**If you have NOT created SSH keys** as it was described in the “Prerequisites” section, you can do it now and import them, or create it via “Create Key Pair”.

**WARNING:** do **NOT** launch your instance without imported/created SSH key, because you will not be able to add it afterwards.

Once you are done with importing yours SSH key, make sure that your key is in the section “Allocated”.

Click on “Launch instance”.

7. On the left menu under the “Network” dropdown menu item go to “Floating IPs”. Click on “Add IP” or something like this (see Fig. 12). Choose the network “147.251.115-PERSONAL”, otherwise it will not work. Click on “OK” and refresh the next screen. You should see your new IP there (Fig. 12).

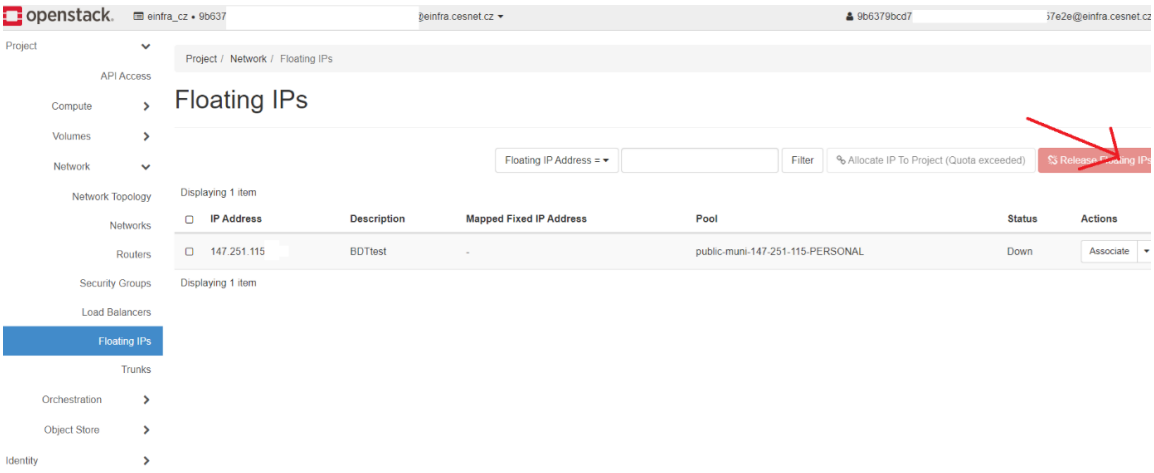


Fig. 12 – Floating IPs settings

8. On the left menu under the “Compute” dropdown menu item go to “Instances” and click on the “Associate Floating IP” button on the right handside (in the red rectangle in the right down corner). In the appeared window assign the IP address as it is show in the Fig. 13.

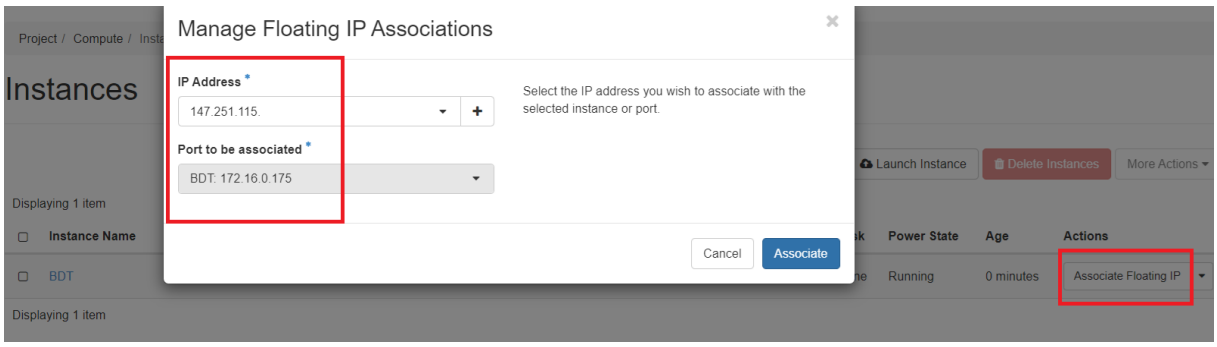


Fig. 13 – Manage Floating IP Associations

9. On the left menu under the “Network” dropdown menu item go to “Security Groups”. Click on “Add rule” and fill the appeared form (Fig. 14):
   - “Rule” – choose “Custom TCP Rule”
   - “Open port” – choose “Port”
   - “Port” – fill it with **22**
   - “Remote” – choose “CIDR”
   - “CIDR” – fill it with your current IPv4-address in the format **<your_IPv4_address>/32**
     (*Tip: if you don’t know your IP-address, just google it* ☺)

- Click on “Add” button

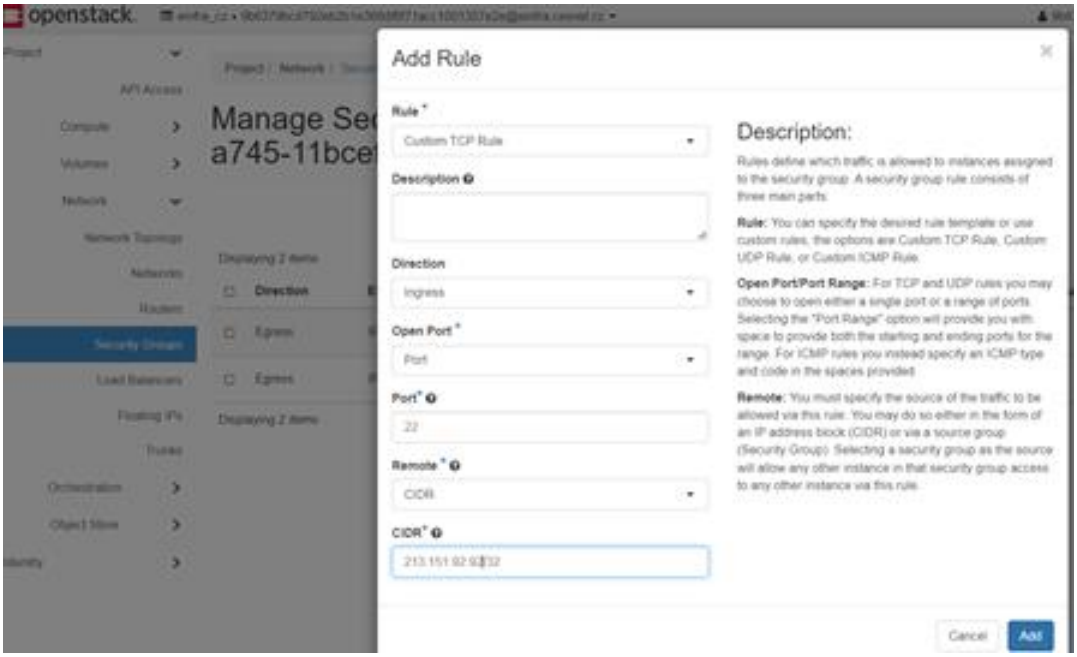


Fig. 14 – Adding a new Security Group rule

10. On the left menu under the “Compute” dropdown menu item go to “Instances”. In your instance in the column “Actions” choose “Edit Security Groups” as it is show in the Fig. 15. In the appeared window assign the created rule to the instance.


Fig. 15 – Assigning a security group to the instance

11. Well done ☺

# Connection

You can connect to the created instance via SSH using Command Line or PuTTY. To connect to your instance use the **second** IP-address in the column "IP-address" on the "Compute"→"Instances" screen (e.g. in the Fig. 15 it is **147.251.115.196**).

USERNAME is **debian**

To connect to your instance you will use your **PRIVATE** SSH key.

## Connect to the Instance via Command Line

1. Open Command Line
2. Put the command (see example in the Fig. 16):
   **ssh -i <path\to\private\ssh\key> debian@<second_ip_address_from_instances>**

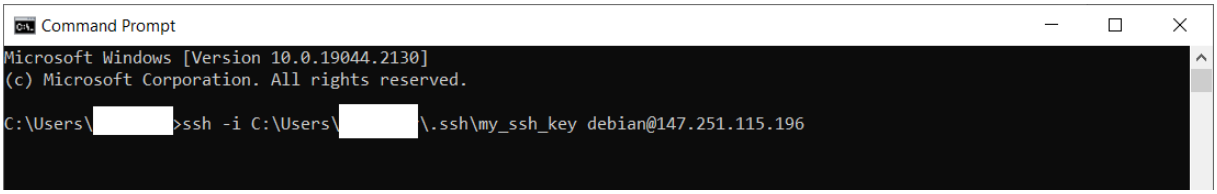


Fig. 16 – Connection to the Instance. Command Line example

## Connect to the Instance via PuTTY

1. Open PuTTY
2. Fill the field "Host Name (or IP address)" with **<second_ip_address_from_instances>**
3. Fill the field "Port" with value **22**

See example in the Fig. 17.

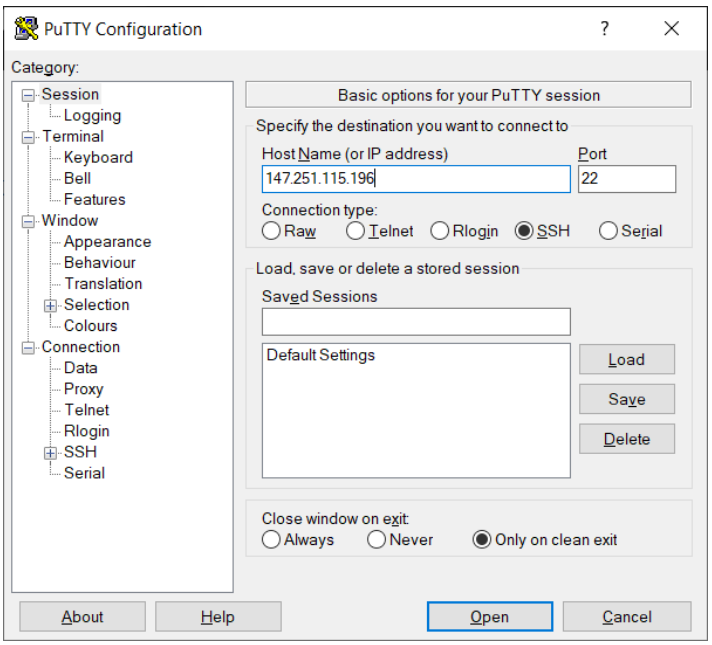


Fig. 17 – SSH connection configuration via PuTTY

4. On the left menu go to “Connection” → “SSH” → “Auth”
5. Click on “Browse” button and choose your PRIVATE SSH key
6. Click on “Open” button to open a connection (Fig. 18)
7. Login as **debian**

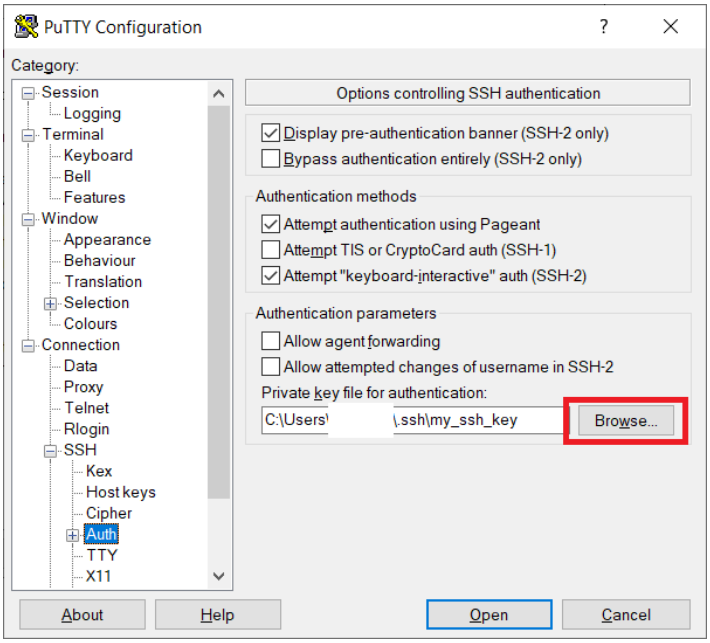

Fig. 18 – Private SSH key configuration