

# How to create Hadoop on your Metacentrum account

## Content

Quick guide.....	2
Manual.....	3
Prerequisites.....	3
Generate SSH via Command Line (recommended).....	3
Generate SSH via PuTTY .....	4
Instance creation .....	6
Connection .....	11
Connect to the Instance via Command Line .....	11
Connect to the Instance via PuTTY.....	11

## 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](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.

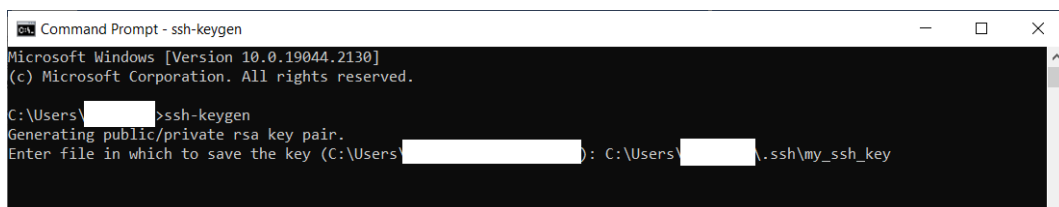
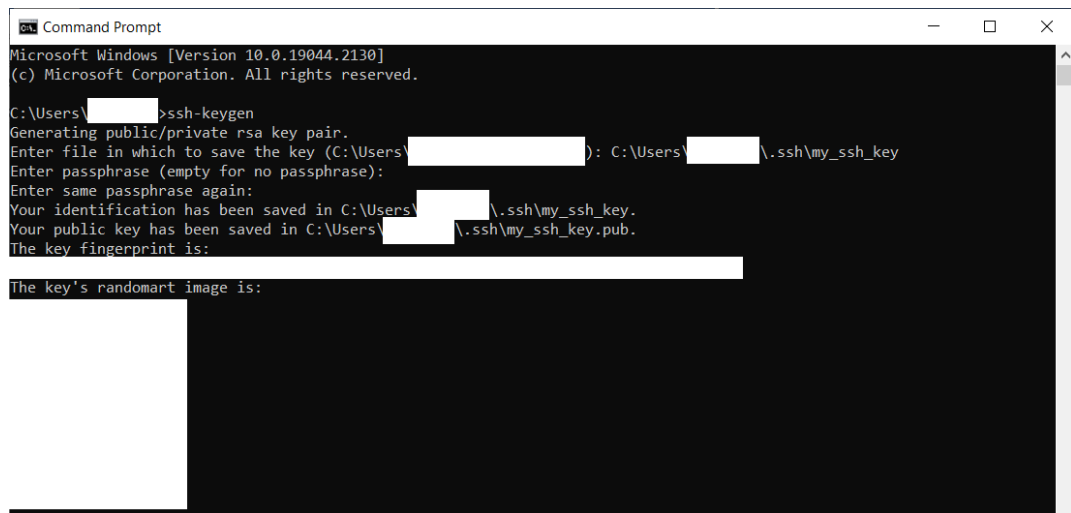


Fig. 2 – ssh-keygen Command Line Interface. Path to save SSH keys

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).



```
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\<username>>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\<username>): C:\Users\<username>\.ssh\my_ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\<username>\.ssh\my_ssh_key.
Your public key has been saved in C:\Users\<username>\.ssh\my_ssh_key.pub.
The key fingerprint is:
<fingerprint>
The key's randomart image is:
<randomart image>
```

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)

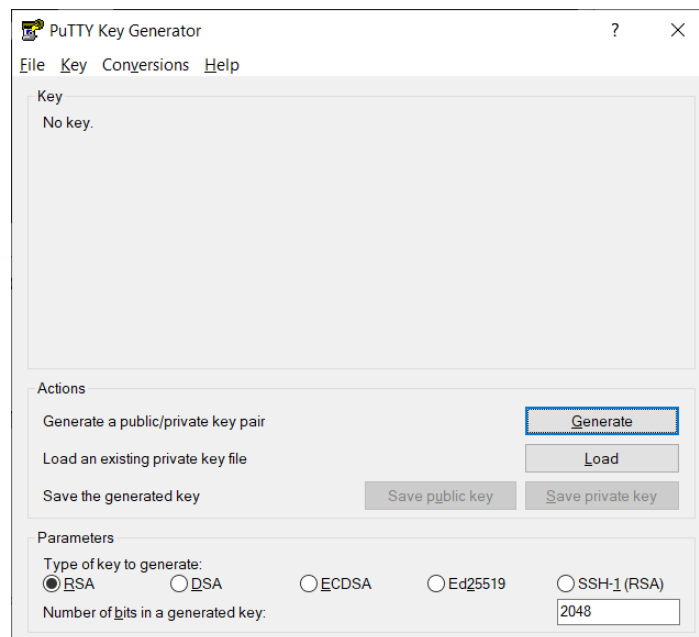


Fig. 4 – PuTTYgen application

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

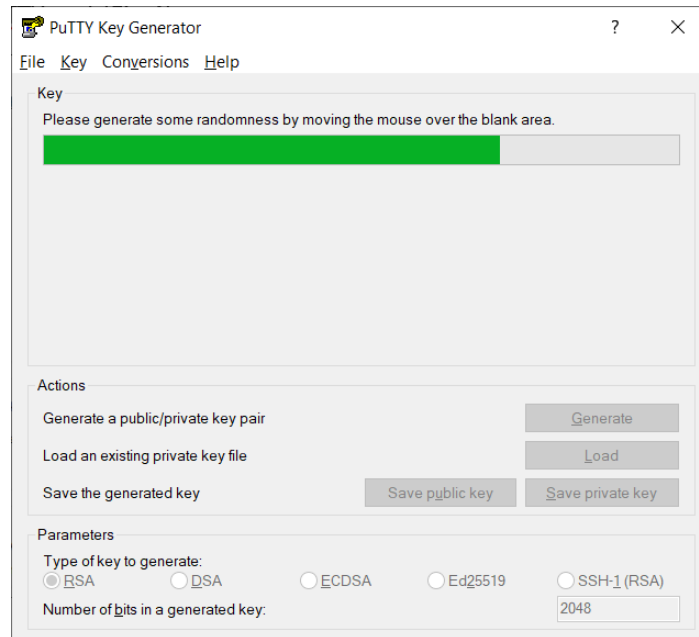


Fig. 5 – Generating SSH keys via PuTTYgen

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).

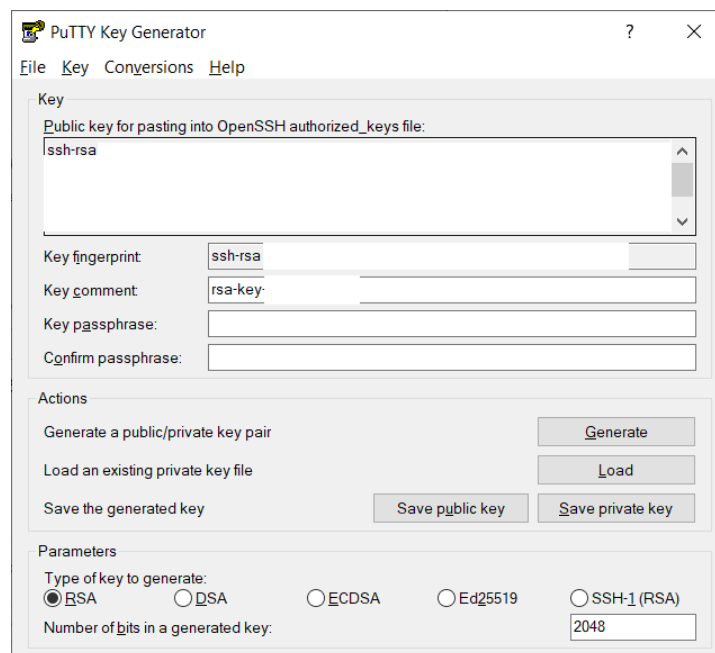


Fig. 6 – Generated SSH keys via PuTTYgen

4. Save your public and private keys in the directory **C:\Users\\.ssh\** using buttons “Save public key” and “Save private key” respectively.
5. Check that your keys are in the directory **C:\Users\\.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”

Launch Instance

**Details**

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

**Instance Name \***  
BDT\_d

**Description**

**Availability Zone**  
brn01

**Count \***  
1

Total Instances (5 Max)  
20%

0 Current Usage  
1 Added  
4 Remaining

**Source**  
Flavour  
Networks  
Network Ports  
Security Groups  
Key Pair  
Configuration  
Server Groups  
Scheduler Hints  
Metadata

Fig. 7 – Instance details

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

Launch Instance

**Source**

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

**Select Boot Source**  
Image

**Volume Size (GB) \***  
80

**Delete Volume on Instance Delete**  
Yes No

**Allocated**

Name	Updated	Size	Type	Visibility
> debian-9-x86_64_hadoop	6/30/21 2:23 PM	4.50 GB	raw	Public

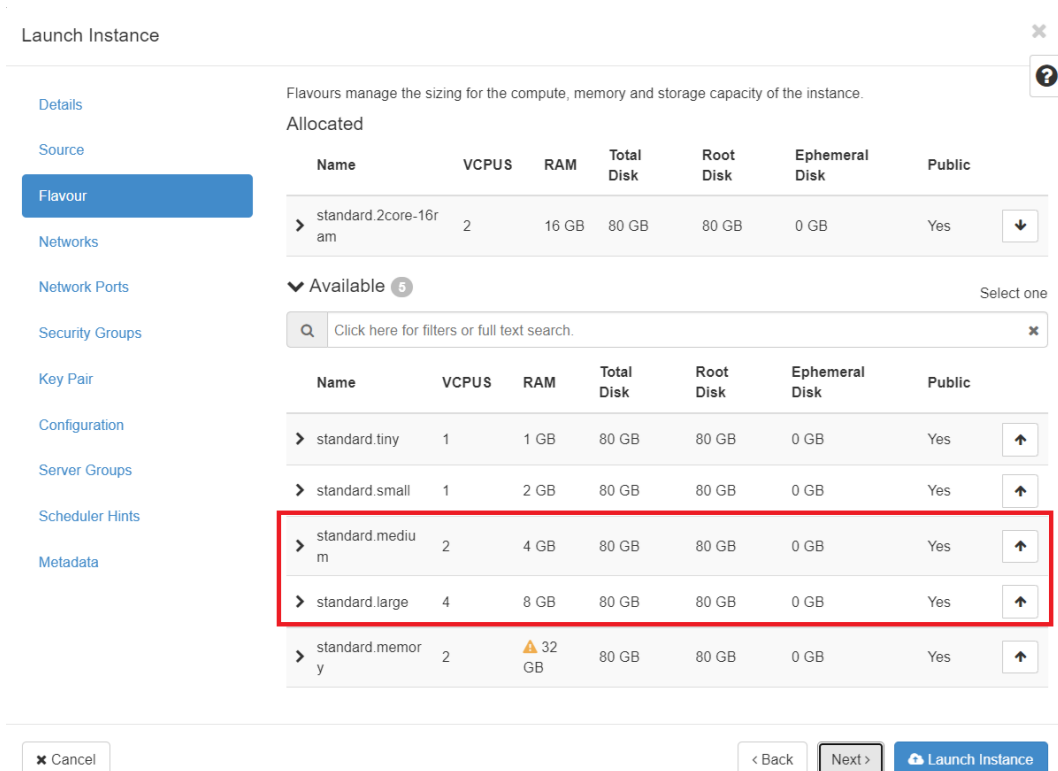
**Available 36**

Search: debian-9-x86\_64\_hadoop

Name	Updated	Size	Type	Visibility
------	---------	------	------	------------

Fig. 8 – Source settings

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



Launch Instance

Flavours manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
> standard.2core-16ram	2	16 GB	80 GB	80 GB	0 GB	Yes

Available 5

Select one

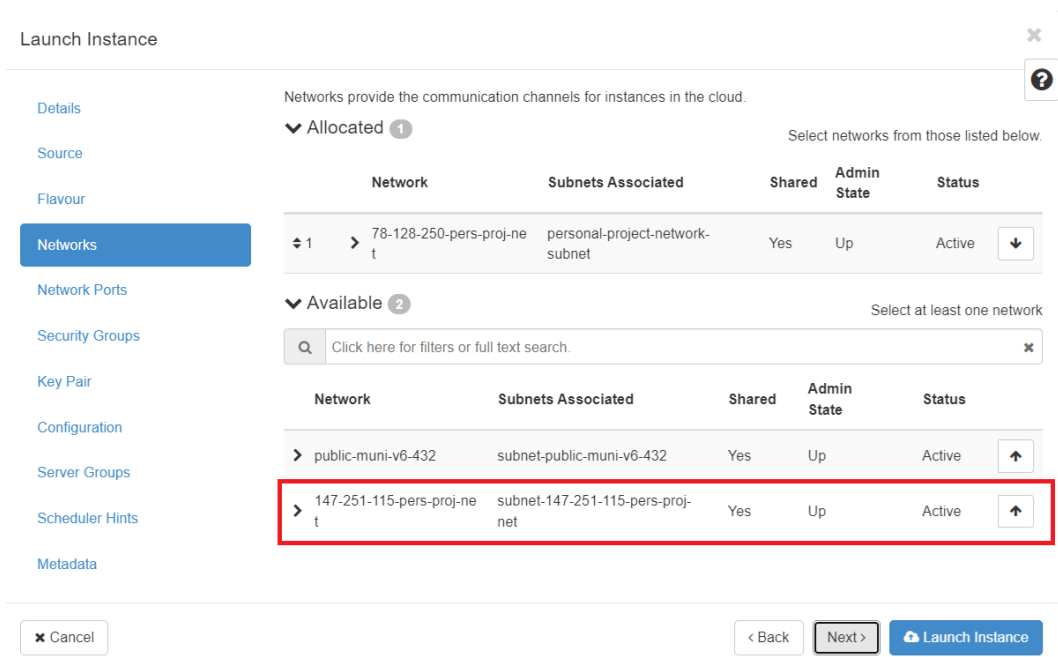
Click here for filters or full text search.

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
> standard.tiny	1	1 GB	80 GB	80 GB	0 GB	Yes
> standard.small	1	2 GB	80 GB	80 GB	0 GB	Yes
> standard.medium	2	4 GB	80 GB	80 GB	0 GB	Yes
> standard.large	4	8 GB	80 GB	80 GB	0 GB	Yes
> standard.memory	2	32 GB	80 GB	80 GB	0 GB	Yes

Cancel Back Next > Launch Instance

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).*



Launch Instance

Networks provide the communication channels for instances in the cloud.

Allocated 1

Select networks from those listed below.

Network	Subnets Associated	Shared	Admin State	Status
> 78-128-250-pers-proj-net	personal-project-network-subnet	Yes	Up	Active

Available 2

Select at least one network

Click here for filters or full text search.

Network	Subnets Associated	Shared	Admin State	Status
> public-muni-v6-432	subnet-public-muni-v6-432	Yes	Up	Active
> 147-251-115-pers-proj-net	subnet-147-251-115-pers-proj-net	Yes	Up	Active

Cancel Back Next > Launch Instance

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).

Launch Instance

Details  
Source  
Flavour  
Networks  
Network Ports  
Security Groups  
**Key Pair**  
Configuration  
Server Groups  
Scheduler Hints  
Metadata

A key pair allows you to SSH into your newly created instance. You may select an existing key pair, import a key pair, or generate a new key pair.

+ Create Key Pair   Import Key Pair

Allocated

Displaying 1 item

Name	Type
> BDT_access	ssh

Displaying 1 item

▼ Available 0

Select one

Click here for filters or full text search.

Displaying 0 items

Name	Type
No items to display.	

Displaying 0 items

Cancel   < Back   Next >   Launch Instance

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”.



- 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).

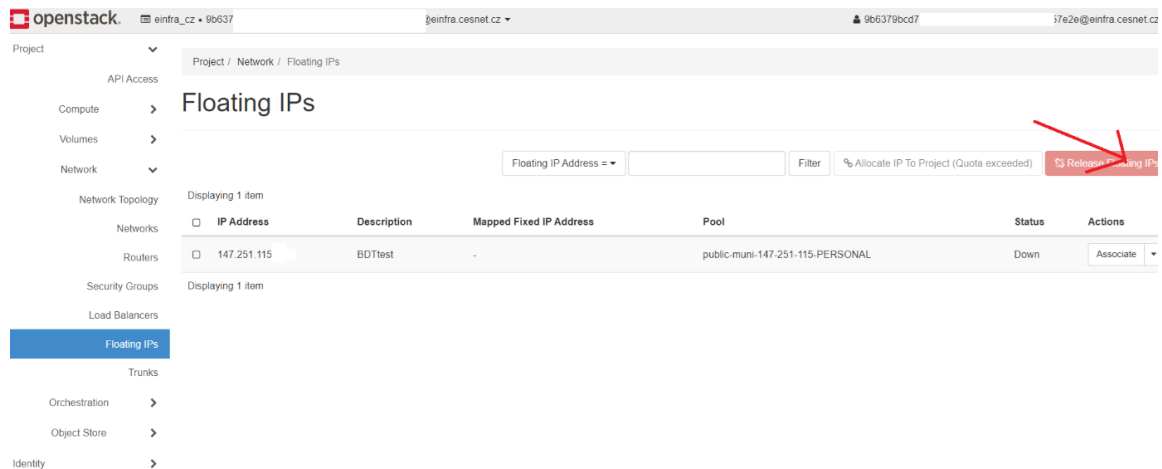


Fig. 12 – Floating IPs settings

- 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.

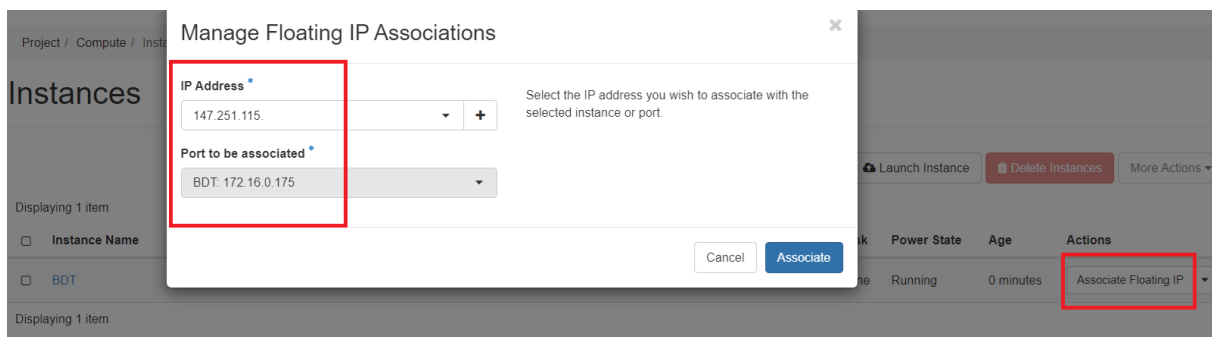


Fig. 13 – Manage Floating IP Associations

- 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

- 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.

### Instances

Instance ID:  Filter Launch Instance Delete Instances More Actions

Displaying 1 item

Instance Name	Image Name	IP Address	Flavour	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
BOT	debian-9-x86_64-hadoop	172.16.100.45, 147.251.115.196	standard2cpu-16ram	BOT_access	Active	eu-west-1	None	Running	15 minutes	Disassociate Floating IP Attach Interface Detach Interface Edit Instance Attach Volume Detach Volume Update Metadata Edit Security Groups

Displaying 1 item

Fig. 15 – Assigning a security group to the instance

- 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>**

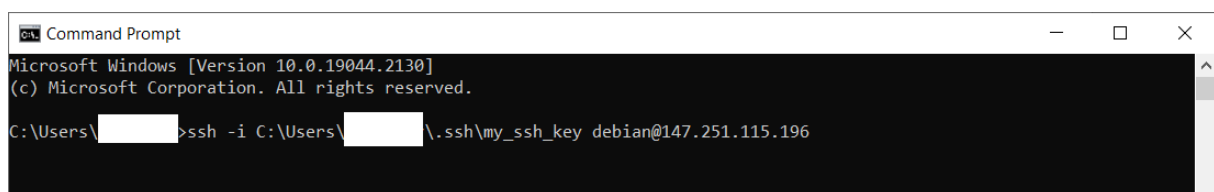


Fig. 16 – Connection to the Instance. Command Line example

### 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.

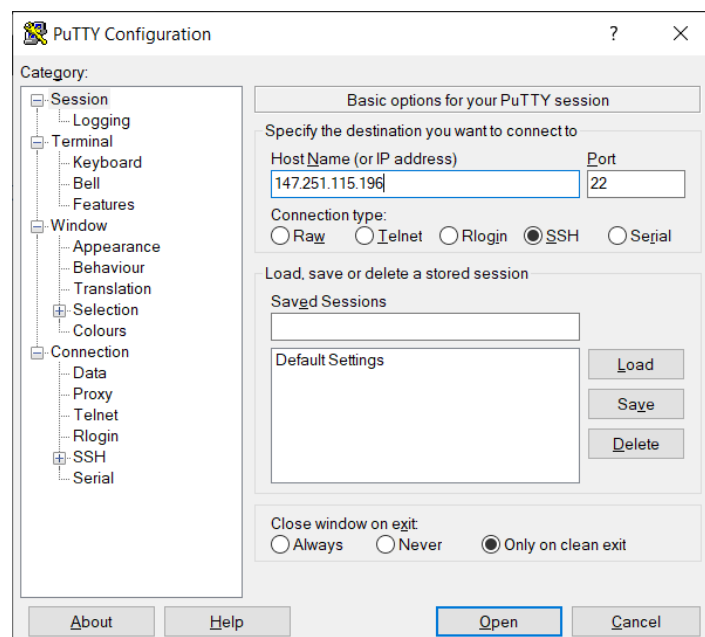


Fig. 17 – SSH connection configuration via PuTTY

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**

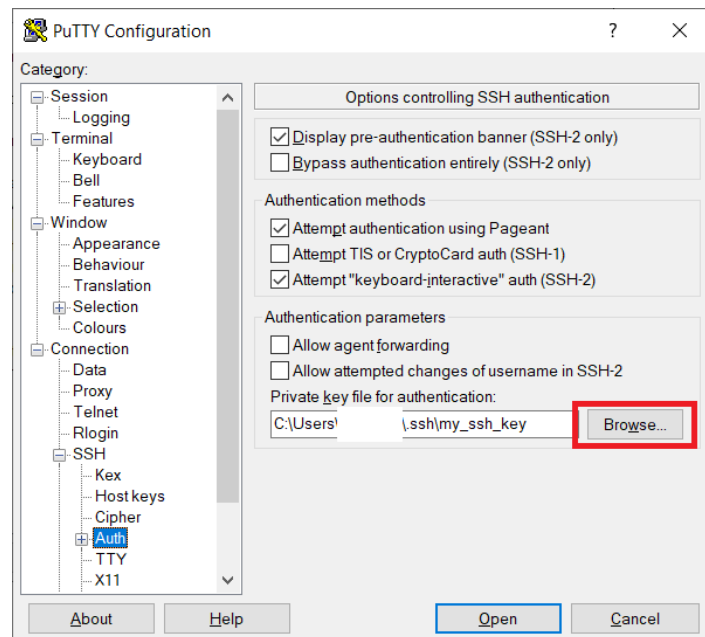


Fig. 18 – Private SSH key configuration