**Exercises, Pouta Cloud Course**

Exercise 1: Creating a temporary Virtual Machine for testing login 1

Exercise 2: Create an SSH key pair for secure login to instance 3

Exercise 3: Create your own Security Group 6

Exercise 4: Create Snapshot 7

Exercise 5: Manage your own volumes 8

# Exercise 1: Creating a temporary Virtual Machine for testing login

1. **Login to cloud dashboard**

* Open a web browser and go to [**http://pouta.csc.fi**](http://pouta.csc.fi)
* Log in with training account provided to you.

1. **Create your cloud machine (with disposable password)**

Navigate to the **Instances** section and click **Launch Instance**

* **Name** it as your *lastname\_firstname\_vm*
* Select **Flavor** as *standard.tiny*
* Select Instance Boot Source as “*Boot from image”*
* Find the image named **Ubuntu-16.04** and select it.
* Navigate to **Access and Security** in same pop-up.
* **Don’t Select any Key Pair**, if it is already selected please deselect it.
* Select predefined security group **SSH** in same pop-up.
* Go to Post-Creation Section in same pop-up
* Select Customization Script Source as Direct Input and add following script data

#cloud-config

ssh\_pwauth: True

password: password1234

chpasswd: { expire: False }

* You can leave the rest as defaults and click on **Launch Instance**

1. **Associate Floating IP to your cloud machine**

To be able to connect to your new instance you need to **assign it a public IP address**:

Go to the **Instances** page

* Find your VM’s name and from the dropdown on the right, select **Associate Floating IP**.
* **Select an IP** from the drop down (if there are no available IPs, click on the **“+”** sign)
* You can see the IP you assigned to your VM in the **Instances** page, next to the name of your virtual machine

To connect to the instance, you will use the **public-IP** address(floating IP) you just assigned.

1. **SSH into your cloud machine**

The CSC images have one user by default: **cloud-user**. This user has no password by default. In the current exercise, you have added post creation instruction to set password authentication on and have changed password of the machine to *password1234.*

You can thus access this machine with password directly without loading any SSH key pairs to your SSH agents.

To connect to your VM from **Windows**, use **Putty**:

* + Open **Putty** and add the **public-ip** you assigned to your VM as the **Host Name (or IP address)**.
  + Click on connect
  + Supply password as *password1234*

To connect to your VM from **Linux or MacOS**, use these commands:

* $ **ssh cloud-user@public-ip**
* Supply password as *password1234*

1. **Exit and Delete your VM**
   * End SSH session from your VM.
   * Navigate to Instances section in cloud dashboard.
   * Select your instance and from extreme right drop down list, click on delete instance.

# Exercise 2: Create an SSH key pair for secure login to instance

When you set up a new virtual machine, you are creating a new “cloud computer” with a specific hardware (Pouta flavors) and an operating system (provided by the image you select). The end result is something similar to what your own desktop computer is, just it is running in the cloud.

In first phase of this exercise, you will create your own cloud machine! To start with you need to follow following steps

1. **Log in to Cloud Dashboard**

* Open a web browser and go to [**http://pouta.csc.fi**](http://pouta.csc.fi)
* Log in with training account provided to you.

Since cloud virtual machines are available via the internet, it very important and necessary to configure different access and security rules. You will start this exercise by setting a basic set of access rules that can be reused to access Pouta virtual machines:

* a Key pair, that you can add to VMs for secure access,
* a Security Group (Set of firewall rules at OpenStack level), to allow access to specific IP addresses.

1. **Create your own SSH key pair**

* Navigate to **Access & Security > Key Pairs**, click on **Create Key Pair**
  + Name it: *lastname\_firstname\_key*

An automatic download will start for SSH key pair. To use your SSH key in **Windows**:

1. You need to first convert the key file to a Windows format. Use **Puttygen** tools to converts your key to *pkk* format (if not installed in your computer, download Putty tools from: <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>)
2. In **Puttygen**, go to **File > Load private key**, and load your *lastname\_firstname\_key.pem* key (note that you have to select **All Files (\*.\*)** in the file browse window to see it)
3. Add a **Key passphrase** and click on **Save private key**, save as *lastname\_firstname\_key.ppk*

To use your SSH key in **Linux** and **Mac OS X**:

1. Create .ssh directory in ~ (the users home directory) if it is not there already

$ **mkdir -p .ssh**$ **chmod 700 .ssh**

1. ... and move the key into it

$ **cd .ssh**$ **mv ../Downloads/lastname\_firstname.pem .**

1. Make the key file read-write only and add a password to it (recommended)

$ **chmod 600 lastname\_firstname.pem**

1. … and add a password to it (recommended)

$ **ssh-keygen -p -f lastname\_firstname.pem**

1. **Create your cloud machine**

To create a new virtual image, you will use an existing Ubuntu 16 image and the access settings you just created.

Navigate to the **Instances** section and click **Launch Instance**

* **Name** it: *lastname\_firstname\_vm*
* Select **Flavor** as *standard.tiny*
* Select Instance Boot Source as “*Boot from image”*
* Find the image named **Ubuntu-16.04** and select it.
* Navigate to **Access and Security** in the same pop-up
* Select **Key Pair** you just created.
* Select predefined security group **SSH** in same pop-up.
* You can leave the rest as defaults and click on **Launch Instance**

Your instance should be visible in the **Instances** tab, wait until it has started. You can check its details by clicking on the name of your instance.

1. **Associate Floating IP to your cloud machine**

To be able to connect to your new instance you need to **assign it a public IP address**:

Go to the **Instances** page

* Find your VM’s name and from the dropdown on the right, select **Associate Floating IP**.
* **Select an IP** from the drop down (if there are no available IPs, click on the **“+”** sign)
* You can see the IP you assigned to your VM in the **Instances** page, next to the name of your virtual machine

To connect to the instance, you will use the **public-IP** address(floating IP) you just assigned

1. **SSH into your cloud machine**

The CSC images have one user by default: **cloud-user**. This user has no password by default so the only way to connect to this virtual machine is via SSH and using this user.

To connect to your VM from **Windows**, use **Putty**:

* + Open **Putty** and add the **public-ip** you assigned to your VM as the **Host Name (or IP address)**.
  + Go to **Connection > SSH > Auth** then add it in **Private key file for authentication** and add the key pair file in ppk format (*lastname\_firstname\_key.ppk*) under
  + You can also connect to your instance with **WinSCP** for transferring files

To connect to your VM from **Linux**, use these commands to add your key to your keys archive:

* $ **ssh-agent /bin/bash**$ **ssh-add lastname\_firstname\_key.pem**$ **ssh -A cloud-user@public-ip**

1. **Play with your cloud machine!**

Now that you have successfully created your own cloud machine, you can start playing with it: install your favorite software package, create some files, run some linux commands etc.

# Exercise 3: Create your own Security Group

Security Group are nothing but OpenStack level firewall rules. In previous exercises you used your pre-defined security group which was allowing SSH connections from all IPs to your machine. In this exercise, you will limit this access to your IP address only by creating an appropriate Security Group.

* To find your computer’s IP address you can visit to <http://v4.ident.me/>.
* Now you can now navigate to **Access and Security** and click on **Create Security Group**, name this security group as your ***lastname\_firstname\_ssh.***
* Click on Manage Rules of your Security Group.
* Add a new rule with **Add Rule**, then select **SSH** from the **Rule** drop down.
* Leave **Remote** as **CIDR**.
* In the **CIDR** field, you should change the default value (0.0.0.0/0) to the IP address you got above (from v4.ident.me). That way connections to your VM are allowed only from your local computer.
* Remember to add /32 IP mask after your IP address.
* Finally Launch your cloud machine with your own Security Group attach.

After attaching this security group your machine would be accessed via IP address you specified in Security Group. In practice, you can play with any set of protocols/ports/IPs for creating your own firewall rules.

# Exercise 4: Create Snapshot

In order to back up a VM state (or to save billing units when a VM is not used) you can create a snapshot from it, so that you can continue later with the same machine. A snapshot can be thought of a version of your virtual machine that can be launch later on as an instance (this instance will be the same as that you have in the moment of taking the snapshot). The snapshots are stored in Pouta as **Images**

1. **Create a snapshot of your machine**

In the Pouta web interface:

* Shut down your instance: **Compute > Instances >** instance\_name **> Shut Off Instance**
* Then, **Compute > Instances >** instance\_name **> Create Snapshot**
* Name it: *lastname\_firstname\_vm\_date*
* This creates a new Image in **Compute > Image**

1. **Review that the snapshot was created properly**

* Go to **Compute > Images**
* Click on the **name of your image (snapshot)** to see its details

1. **Delete your machine**

* Go to **Instances**
* Click on your instance and delete it.

1. **Relaunch new instance with same state**

Navigate to the **Instances** section and click **Launch Instance**

* **Name** it: *lastname\_firstname\_vm*
* Select **Flavor** as *standard.tiny*
* Select Instance Boot Source as “*Boot from Snapshot”*
* Find your Snaspshot and select it.
* Navigate to **Access and Security** in the same pop-up
* Select **Key Pair** you created.
* Select Security Group you created in same pop-up.
* You can leave the rest as defaults and click on **Launch Instance**

This will launch new cloud machine which is in same state as of instance you deleted.

# Exercise 5: Manage your own volumes

You can add additional volumes to your cloud machines. In this exercise, we will learn how to add additional volume to instance. Volumes are like your virtual hard disks, you can save data in them and reattach to any other instance of your choice.

1. **Create your volume.**

* Navigate to Volume section.
* Click on create volume, name volume as your **lastname\_firstname\_vol** and size as 10GiB

1. **Attach your volume to instance.**

* After creating volume, click on manage volume.
* Attach volume to your instance.

1. **Mount your volume.**

* Connect to your cloud virtual machine.
* Check disk partition using fdisk command and find your volume
  + **$ sudo fdisk -l**
* Create file system of your choice on your volume, xfs or ext4 give good performance in pouta. Remember to enter correct path for volume based on output from fdisk command you executed above.
  + $ **sudo mkfs.xfs /dev/vdc1**
* Mount your volume to instance’s file system
  + $ **sudo mount /dev/vdc1 /media/volume**
* Once you have mounted your volume you can start using in it. In case you want to detach volume, you should unmount it first, you can do so by
  + $ **sudo umount /dev/vdc1**