Exercises: Pouta Cloud Course, Autumn 2018

Exercise Set 1:

Exercise Set 2 (Atleast 3 of Following Excercises):

Exercise 1: Creating a temporary Virtual Machine for testing login

A. Login to cloud dashboard

- Open a web browser and go to **https://pouta.csc.fi**
- Log in with training account provided to you.

B. Create your cloud machine (with disposable password)

Navigate to the **Instances** section and click **Launch Instance.** (Please note Cloud Instance = Cloud Virtual Machine)

- **Name** it as your *lastname_firstname_vm*
- Select **Flavor** as *standard.tiny*
- Select Instance Boot Source as "*Boot from image*"
- Find the image named **CentOS-7** 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-World** 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**

C. 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.

D. 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** based machines, 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**, based machines use these commands:

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

E. 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 instance" with specific:

- Compute resources & hardware (Based on Pouta flavors you choose),
- Operating system (Based on OS image you select)
- Access configurations (Based on Security Groups & SSH Key pairs you create)

The end result is a new vanilla server with desired resources, hardware, OS & access configurations running remotely in CSC's datacenters.

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

A. Log in to Cloud Dashboard

- Open a web browser and navigate **https://pouta.csc.fi**
- Log in with training account provided to you.

Since cloud virtual machines are accessible 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.

B. 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** based machine:

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: http://putty.tx.se/latest.html or 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** based machines:

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

```
$ cd ~
$ mkdir -p .ssh
$ chmod 700 .ssh
$ mv keyname.pem .ssh
```

2) ... and move the key into it

```
$ cd .ssh
$ mv ../Downloads/lastname_firstname.pem .
```

3) Password protect the key (recommended but not necessary)

```
$ ssh-keygen -p -f keyname.pem
```

4) Make the key file read only.

```
$ chmod 400 lastname_firstname.pem
```

C. Create your cloud machine

To create a new virtual machine, you will use an existing CentOS-7 OS image and the access configurations 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 **CentOS-7** and select it.
- Navigate to **Access and Security** in the same pop-up
- Select **Key Pair** you just created.
- Select predefined security group **SSH-World** 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.

D. Associate Floating IP to your cloud machine

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

E. SSH into your cloud machine

The CSC OS images have a sudo user by default: **cloud-user**. This user has no password by default, so the only way to connect virtual machines running with CSC OS images is via SSH using cloud-user.

To connect to your VM from **Windows** based machine, 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** based machines, 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**

F. Celebrate the success!

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..

Finally, install telnet and enjoy Star Wars show!

- $ **sudo yum install telnet**
  $ **telnet towel.blinkenlights.nl**

Exercise 3: Create your own Security Group

A Security Group is OpenStack level firewall rules. In previous exercises, you used your pre-defined security group which was allowing SSH connections from whole internet to your cloud instance. In this exercise, you will limit this access to your IP address only by creating an appropriate Security Group. We would begin the exercise by creating a wrong security group which will restrict you from accessing your cloud instance. Then we correct the security group which allows you to access your cloud instance.

Create Wrong Security Group

- Find your machine'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 any valid IPv4 address ***except*** the one you got from above (from v4.ident.me). Remember to add /32 IP mask after the IP address.
- Save your Security group
- Edit Security Group attached to your VM by clicking **Edit Security Groups** dropdown which is on right side of your VM name in the **Instances** page. Remove **SSH-World** security group by clicking **"-"** and add security group you created by clicking **"+"**
- Try to SSH again to your VM, You should not be able to get in as with your new security group definition you have restricted firewall access to a IP which your machine doesn't have.

Correct your Security Group

- On WebUI go to **Access & Security/Security Group,** Find your security group and click on **Manage Rule**s, delete the SSH firewall rule you created in above steps.
- Click on **+Add Rule** , then select **SSH** from the **Rule** drop down. This time in CIDR field put IP address you got above (from v4.ident.me). That way connections to your VM are allowed only from your local machine's IP.
- Remember to add /32 IP mask after your IP address and click **Add**.
- Try to SSH again into your machine, you should be able to get in ☺

In practice, you can play with any set of protocols/ports/IPs by creating your own firewall rules in security groups.

Exercise 4: Install Docker CE & run RStudio server in Docker Container

For instructions please visit Pouta Object store:
https://object.pouta.csc.fi/pouta-autumn-course-2018/install_Rstudio_docker_container.txt

Exercise 5: Build your own RStudio Server on your Cloud Instance

For instructions please visit Pouta Object store:
https://object.pouta.csc.fi/pouta-autumn-course-2018/pouta-recipies.html

Exercise 6: Installing software with Conda

For instructions please visit Pouta Object store:
https://object.pouta.csc.fi/pouta-autumn-course-2018/pouta-recipies.html

Exercise 7: Installing Stacks server in Ubuntu VM

For instructions please visit Pouta Object store:
https://object.pouta.csc.fi/pouta-autumn-course-2018/pouta-recipies.html

Exercise 8: Install OpenStack CLI client & Use it

For instructions please visit Pouta Object store*:*
https://object.pouta.csc.fi/pouta-autumn-course-2018/use_OS_client.txt

Exercise 9: Create Snapshot

In order to create copy of your cloud instance's OS, middleware, runtime configurations or application stacks you build inside it, you can create a snapshot of VM. Snapshots also provide means to capture and store filesystem state of your instance.

You can share snapshots with other Pouta users or use it for yourself to launch new VM's with same configurations, applications & file system state. Snapshot also provide you mechanisms for saving billing units inside Pouta clouds, for ex. You can take snapshot of your ideal machine, delete the ideal machine & relaunch a new instance with the snapshot.

The snapshots are stored in Pouta as **Images**

A. Install some applications & save some data in your VM

In your VM:

- Install some software packages of your choice on your VM
    - $ **sudo yum install <your-software-package>**
- Create & Save some files

B. 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**

C. Review that the snapshot was created properly

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

D. Delete your machine

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

E. 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. Please verify if you still have your data and installed packages in VM. Notice that your VM's private IP is now different.

Exercise 10: Manage your own volumes

For instructions please visit Pouta Object store:
https://object.pouta.csc.fi/pouta-autumn-course-2018/mount_volume.txt

Exercise 11: Create your own Bucket & Object using WebUI

A bucket (also called container in some object storage environments) is a storage compartment for your data and provides a way for you to organize your data. You can think of a bucket as a folder in

Windows® or a directory in UNIX®. The primary difference between a bucket and these other file system concepts is that containers cannot be nested. Data must be stored in a bucket so you must have at least one container defined in your account prior to uploading data.

Note: A Public bucket will allow anyone with the Public URL to gain access to your objects in the container.

- Navigate to **Object Store** section and click on **Containers** in Pouta WebUI.
- Click on **+Container** icon and name your container or bucket as **YYYYMMDD-yourlastname.** (YYYYMMDD is today's date)
- Check Public access check box and create your bucket.
- Create a text file on your local machine, Add some random lines of content in it or "Hello World from Object store" atleast, save this file as **yourlastname.txt.**
- Upload this file to bucket, This file will be treated as a Object by Pouta Object Store.
- Since bucket is public, all of its contents would be public by default and can be accessed over HTTPS using Public URL of your object.
- You can access contents of your object over HTTPS by browsing its public URL which is ***https://object.pouta.csc.fi/$Your-Bucket-Name/$Your-ObjectName*** which for this exercise would be ***https://object.pouta.csc.fi/YYYYMMDD-yourlastname/yourlastname.txt***

You can browse above URL in your browser or Curl it to on terminal to see its contents.

Exercise 12: Upload Object to your Bucket using s3cmd client

For instructions please visit Pouta Object store:

https://object.pouta.csc.fi/pouta-autumn-course-2018/uses3cmd.txt