How to get Access to CSC Cloud Resources – and Create a Virtual Machine

In an old paper factory in Kajaani, Finland, there lies the CSC data center. Wrapped by OpenStack, the computing infrastructure offers a variety of cloud resources to researchers and students in Finland, and in whole Europe.

Image Source: CSC.fi

CSC (the IT Center for Science) has a catalogue of cloud services, however, for this course, we will be mostly utilizing **cPouta**, which offers you internet-accessible virtual machines, the control over their networking, such as virtual networks and floating IPs. It is closely related to AWS's EC2 (Elastic Compute Cloud), and Azure's Azure Virtual Machine.

cPouta Web Interface – How to Make an Account and Get Access

The cPouta web interface is used to create virtual machines in CSC. To get access to CSC resources, students need to sign up on CSC using Haka authentication method, using their Tampere University credentials.

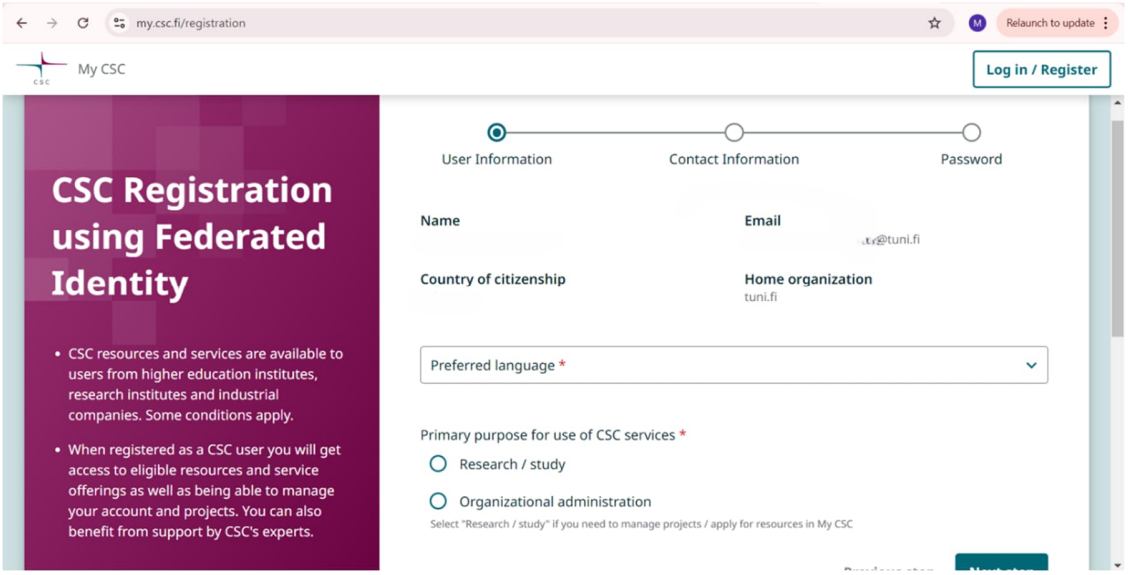
Step-by-Step Instructions to Get Access to CSC

1. TUNI x CSC Auth: Go to CreateAccount , and select the Haka authentication.

2. Select “Tampere Universities” from the drop-down list.

3. You will be asked to login via your TUNI credentials, so, do that. After successful authentication, click “accept” the CSC service to connect with your TUNI account.

4. Successful authentication will take you to the CSC Sign Up page. Since we are not using CSC for business purposes, you will select “Research/Study” and click next.



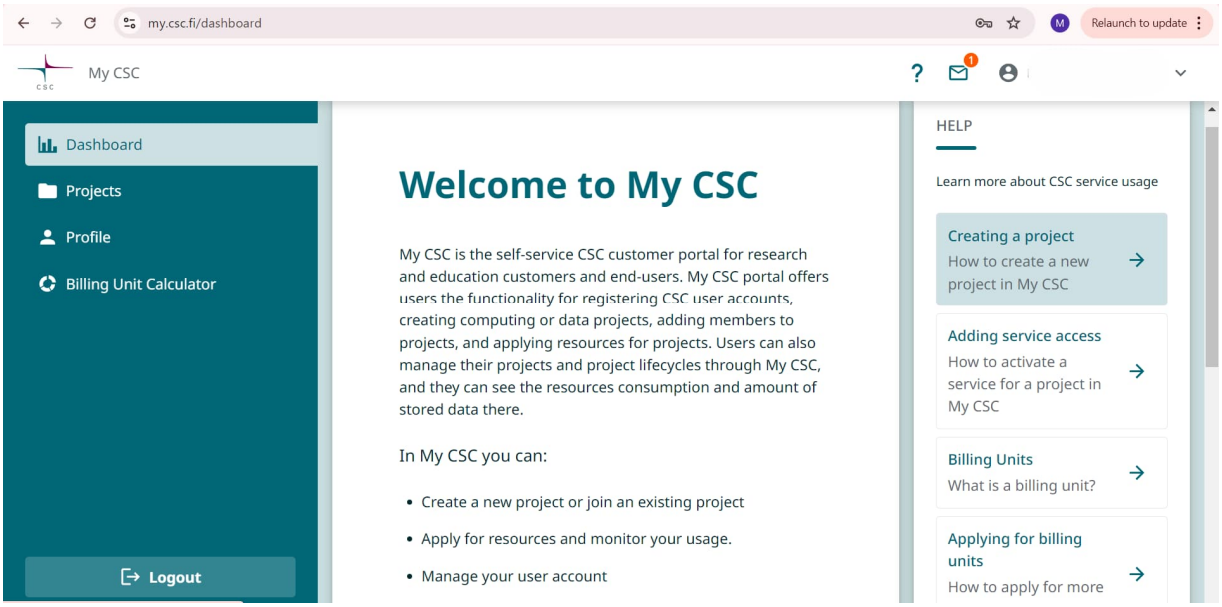
This Sign-Up page will ask for your personal information, so please fill out the required information. You will get a confirmation email from CSC, use the link in the email and set up a CSC-password.

NOTE: There are two ways to login to CSC: using Haka (+ Tuni creadentials) or using CSC-login and password. Haka login is preferred, so you should not need to use this CSC - password unless you are not able to use Haka login.

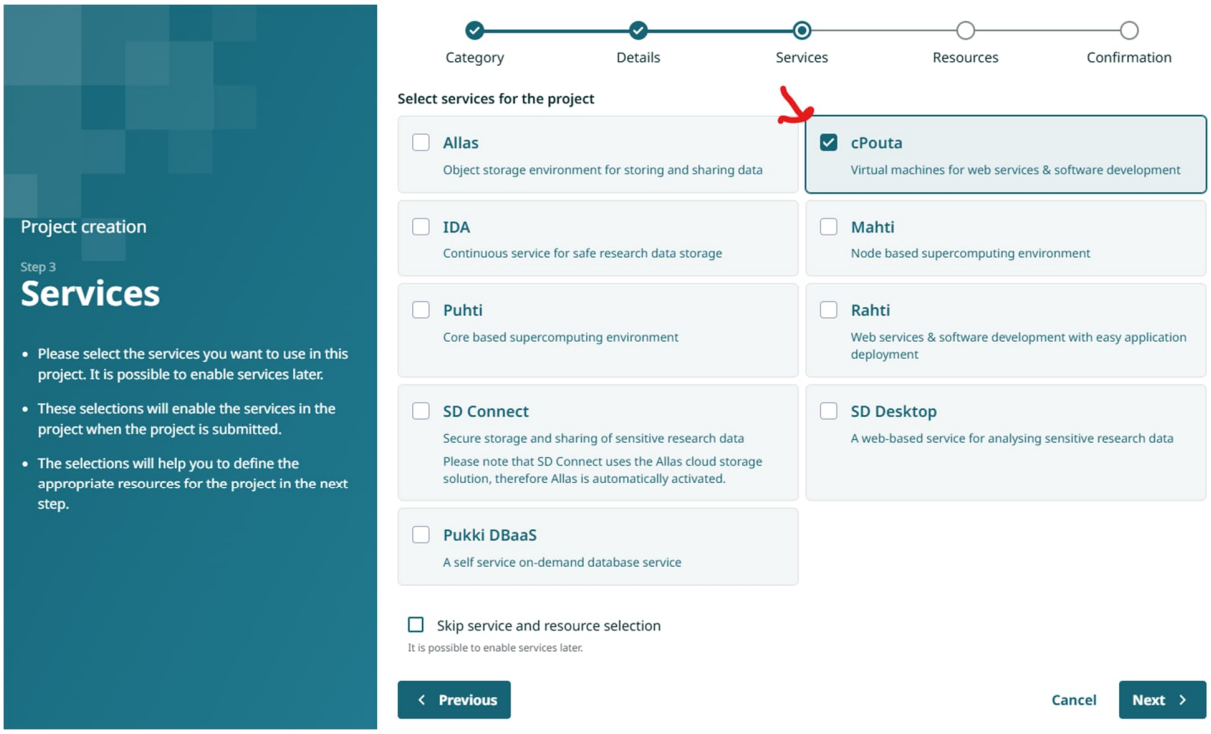
NOTE: If you have problems with setting the password (link is too old), you can ask for a new link via https://my.csc.fi/forgot-password (your CSC username in in the email).

5. After successfully signing up open https://my.csc.fi and login using Haka (+ Tuni credentials).

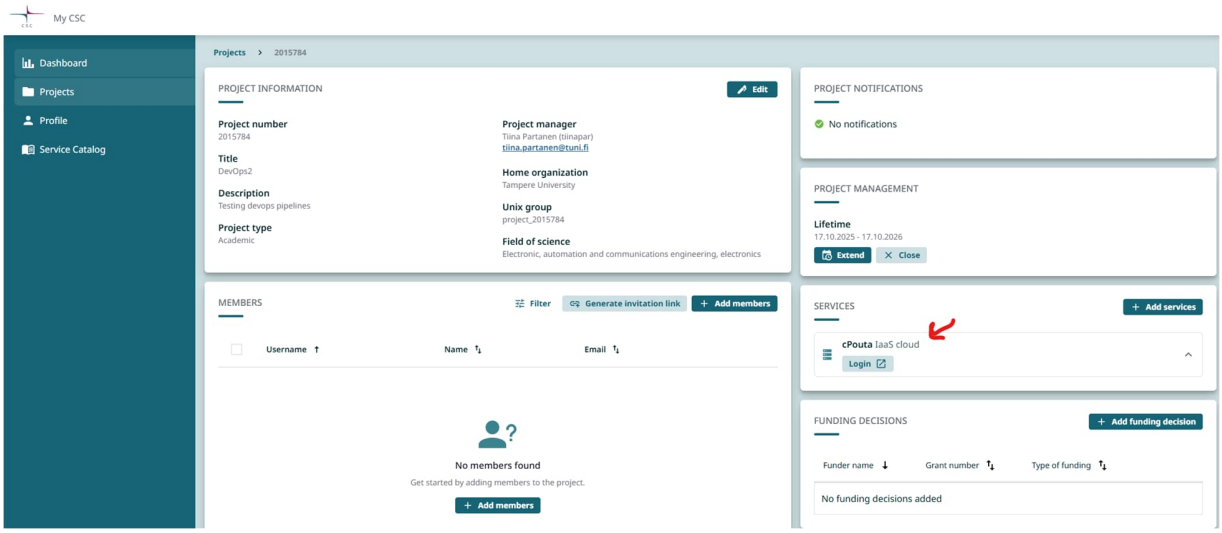
   You will be taken to the CSC dashboard. At this point, you do not have access to any services, such as cPouta. To do that, you need to apply for access to the service, so, let's do that.



   On the left, click on “Projects,” and create a new project. Fill in the requested information and select cPouta – service (“base”-package) for your project:



It may take up to 30 min to get the service activated but after that, you will see that you are part of a new project, where you are the project manager and you have cPouta-service.



Launch Your First Virtual Machine on CSC

After getting access to CSC, making a project, and adding the cPouta service in your project, it is now time to create a virtual machine. Select cPouta Login or go to https://pouta.csc.fi , and sign in using Haka (+Tuni credentials) .

Step 1. Create a Key Pair in the Web Interface:

1. Go to **Compute > Key Pairs** in your cloud interface.
2. Click **Create Key Pair** and give your key a name (Key Type: SSH Key).
3. A file (e.g., `keyname.pem`) will be downloaded to your computer. **Save this file carefully**—you won't be able to download it again. This file is used to access your server later.

Step 2. Move and Set Permissions for the Key (Linux/Mac):

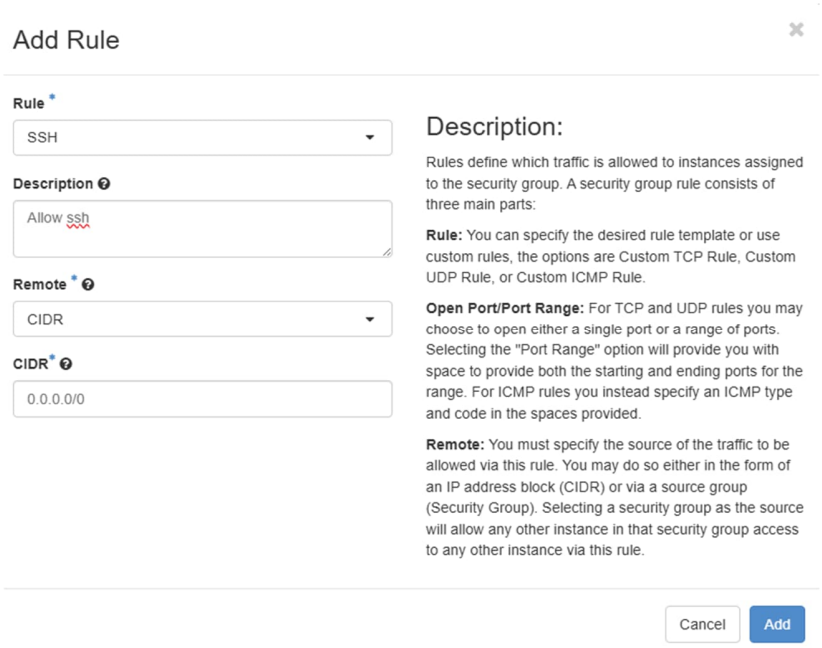
```
1. mkdir -p ~/.ssh  # Create the .ssh directory if it doesn't exist
2. chmod 700 ~/.ssh  # Set the directory's permissions (owner-only access)
3. mv ~/Downloads/keyname.pem ~/.ssh  # Move the key to your .ssh folder
4. chmod 400 ~/.ssh/keyname.pem  # Make the key readable only by you
```

Now your key is ready to to be used for SSH connections! Detailed Instructions can be found here.

Step 3: Create a Security Group

1. In the cPouta dashboard > Network > Security Groups, create a new security group, name it for example DevOps, and click "Create Security Group" (You will see that only Egress (Outgoing) traffic is allowed, meaning you can access the internet, no port is open yet.)

2. Click on “**Add Rule**”, and from the first drop down menu, select SSH, and leave the other fields as they are, and finally, click “Add”. Your SG is created.



(by default, the CIDR range is 0.0.0.0, meaning anyone from the internet can access your VM via port 22 (SSH). This is not a good practice in production systems, however, for simplicity and ease, let’s leave it that way.)

If you want to open more ports, such as 443 for HTTPS connections, you can do so by repeating step 2 and selecting the corresponding port. (Detailed Instructions)

Step 4: Launch a Virtual Machine

1. In the cPouta dashboard > Instance > Launch Instance.

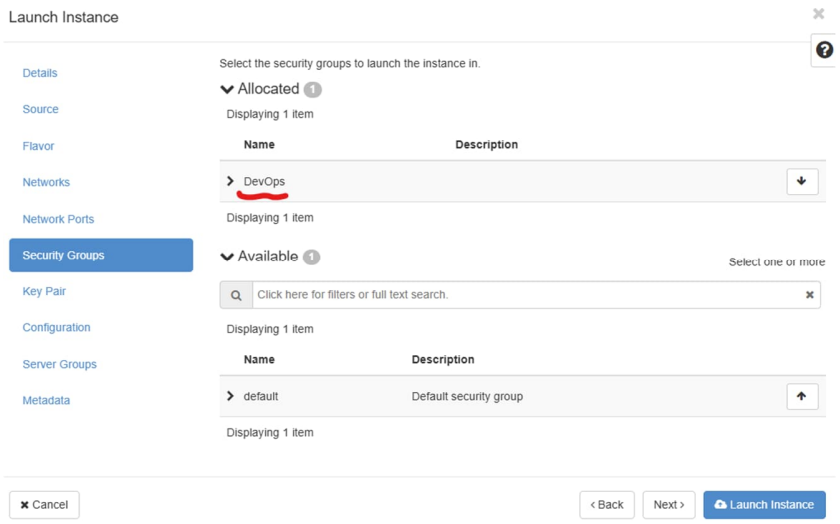
2. Set the following:

    a. **Details → Instance name**: Choose a name for your VM.

b. **Source**: Select `Ubuntu-22.04` as the operating system.
c. **Flavor**: Choose `standard.small`.
d. **Security Groups:** Select the **DevOps** security group you created earlier.
e. **Key Pair**: Select the **SSH key pair** you created earlier,

and finally,

click **launch**.

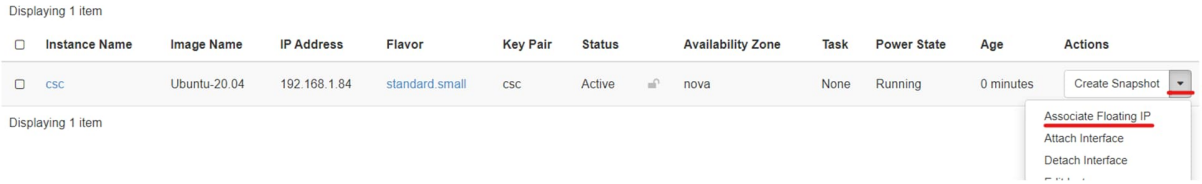


NOTE: Use the little arrows (up/down) to select items.

Step 5: Assign a Public IP (Floating IP)

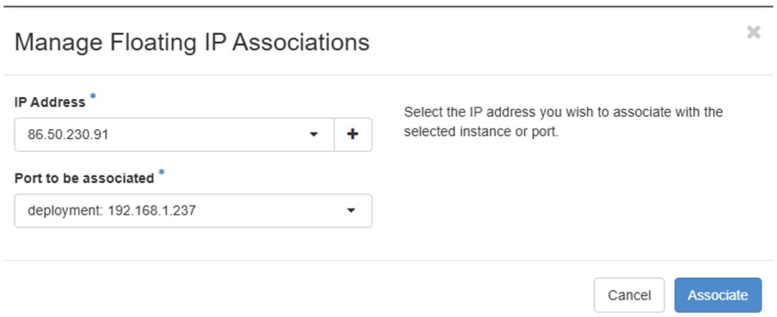
1. Once the VM is launched, it will only have a private IP. You need to allocate a public IP addres for it from the pool of Floating IPs.

2. In the "Actions" column > down arrow (˅) drop down > Associate Floating IP



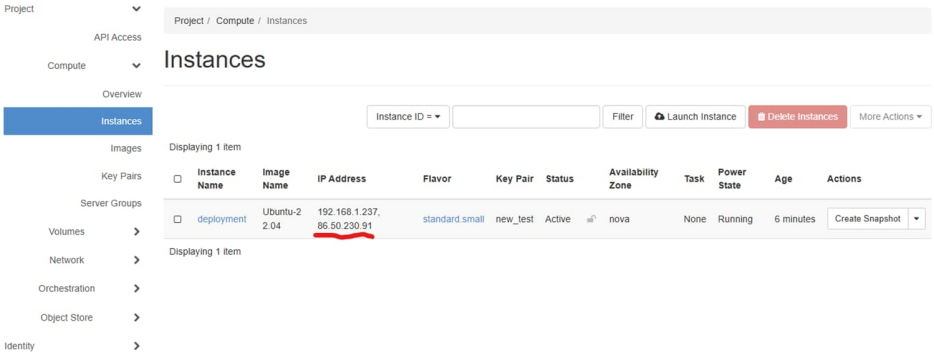
3. In IP Addresses, click on Plus sign at the right, and create a new Floating IP from the pool, and then click on Allocate IP.

4. Then associate the new IP address with your server by selecting the virtual machine's private IP and the newly created public IP and click "Associate".



Step 6: Connect to Your Virtual Machine

1. Note the **floating IP** of your VM from the cPouta web interface.



2. Open an SSH connection to the VM using your private key:

```
ssh -i ~/.ssh/ your_keyname.pem ubuntu@your_floating_ip
```

Now you can log in to your virtual machine!

You are responsible for the security of the virtual machine,

Note: Sometimes, based on the machine and operating system you are using to connect to a VM via SSH, some permission errors can occur. To avoid such errors, you can consult the official CSC documentation for creating a VM from the Web UI.