Quick Start Guide to Compute Canada Cloud Service

Launching your first instance (VM)
Login to the East or West cloud
Dashboard
SSH key pair
Importing an existing key pair
Creating a new key pair
Launching a VM
Network
Private IP
Public IP (assign a public IP)
Firewall, add rules to allow SSH
Connecting to your instance with SSH.
Where to go from here

Launching Your First Instance (VM)

Login to the East or West Cloud

Simply go to https://east.cloud.computecanada.ca or https://west.cloud.computecanada.ca, depending on which cloud you want to launch your instances, and enter your WestGrid credentials.

After you have successfully logged in, you are presented with the dashboard. From here you can see an overview of the resources you are using.

When your tenant (project) is created, most of the configuration is done at the same time.
SSH Key Pair
When starting an instance, there is no password for admin or root account on your server. You can only authenticate to your server with an SSH key. You can either import your SSH key in openstack, or you can create a new one.

In order to manage your Key Pair, click on “Access & Security” from the left menu, then on the “Key Pairs” tab.
Importing an Existing Key Pair

Click

Then,
1. Give a name to your key.
2. Paste your public key.
3. Click on the blue Import Key Pair button.
Creating a New Key Pair

Click

Then,

1. Give your key a name.
2. Click on the blue Create Key Pair button.
3. Save the <key name>.pem on your disk.

On UNIX hosts, you will need to “chmod 400 <key name>.pem” in order to connect later on (This need to be done on your machine, not the VM).

Launching a VM

To launch an Instance, simply click on Instances menu on the left, then click

You are now presented with a form to define your Instance.

Details Tab

Instance name: test
This is the name of your instance.
Flavor: c1-3.75gb-36
The flavor name defines the specs of the VM. This particular flavor has 1 vcpu, 3.75 GB of ram and an Ephemeral disk of 36GB,
Instance Count : 1
Instance Boot Source: Boot from image
Image Name: CentOS-7-x86-64-GenericCloud-1503

Access & Security Tab
This is where you select your SSH Key Pair. If you have only one, it will be selected by default. You can also select which security group to add to your instance.

Networking Tab
Select which network to connect to. You do not need to change this now. Networking will be discussed below after you have launched an instance.

Post-Creation Tab
This allows you to add a configuration script. This is where you can paste a cloud-init script.

Once you have defined your instance, click on the blue Launch button and your instance will be created. The instance you just defined is going to appear in the instance list. It will proceed through different tasks and then start, depending on a variety of factors, it can take up to a few minutes for your instance to start. You will see some information on your instance.
Note: When creating a persistent service, we recommend that you boot your instance from a volume.

**Network**

**Private IP**
On the Instance list, you will see the IP addresses to which your Instance are linked. By default a network on 192.168.X.0 is created for your tenant. You can see the private IP your Instance has on the Instance list screen. You can use this IP to communicate with other Instances you have started.

**Public IP (Assign a public IP)**
To assign a public IP, you need to select “Associate Floating IP” from the More button of the Actions column.

Since your tenant is new and hasn’t used an IP address yet, you need to click on the “+” sign to allocate an IP. (Since there is only one pool of public address, it should be already selected.) Then click on the blue Allocate IP button.

The public IP will appear on the IP Address field, and the port to which it should be nated should already be selected. Simply click on the blue Associate button.

Note that the public IP is **NATted (Network Address Translation)** to the private IP of your instance.
Firewall, Add Rules to Allow SSH

In order to be able to connect to your instance via SSH, you will need to allow SSH to get through.

Go to “Access & Security”, in the “Security Groups” tab, then on the default row click

![Manage Rules](image)

On the next screen, click

![Add Rule](image)

For SSH, there are already predefined rules. Simply select SSH in the Rules drop down menu, then under Remote, keep CIDR.

If you know which address you are connecting from, type it in the CIDR text field; otherwise keep 0.0.0.0/0. This will allow the whole world to connect to your server via SSH.

Finally, click the blue Add button.
Connecting To Your Instance With SSH.
If you created a key pair on the first step, you will need to know where it is.

    ssh -i /path/where/your/key/is/my_key.key username@<public IP of your server>

Most common Linux distributions have standardised on the name of the distro as the username. To connect to the provided CentOS images, you would use:

    ssh -i /path/where/your/key/is/my_key.key centos@<public IP of your server>

Ubuntu instances have the username “ubuntu”; Debian ones are “debian”.

By default the preconfigured cloud username will have full sudo privileges. The root account is normally disabled.

You are now connected to your instance.

Where To Go From Here
Openstack upstream documentation:  http://docs.openstack.org/icehouse/
CLI control:  http://docs.openstack.org/developer/python-openstackclient/
WestGrid documentation:  https://www.westgrid.ca/support/quickstart/CC-Cloud