_____

_____

_____

Due Date: Wednesday, October 6th

PROJECT GOAL

The objective of this assignment is to interface with OpenStack's CLI to authenticate to the system and launch a VM. Mastery of these steps would enable one to develop software to manage and configure a cloud system without using the dashboard.

OVERVIEW

OpenStack consists of several service components that *listen* to specific ports on the CS Cloud. Using the common OpenStack CLI you will create a VM and log into said VM.

PROJECT REQUIREMENTS

Requirement	Completion (To Be Verified by Instructor or TA) *Grader Comments*
1. Obtain an keys for instance and set keypair	*10 points*
2. Create security group with ICMP and SSH enabled	*5 points*
3. Create a VM Instance	*5 points* *You should be able to go to your dashboard and see your new VM, if successful*
4. Login to your new instance using the IP and SSH keys.	*5 points*

STEP 1: CREATE AND SOURCE ENVIRONMENT FILE

LINUX

1. Log into the CS Manage node or Linux computer.
    a. If you use a Linux computer you will need to setup the environment described below. Also you will need to change the OS_AUTH_URL to use the controller's IP address.
2. Copy over or create openrc.sh file.

```
export OS_USERNAME=<team username>
export OS_PASSWORD=<team password>
export OS_PROJECT_NAME=<team username>
export OS_IDENTITY_API_VERSION=3
export OS_AUTH_URL=http://controller:5000/v3/
export OS_PROJECT_DOMAIN_ID=default
export OS_REGION_NAME=RegionOne
```

3. Source the environment file.
   source openrc.sh

STEP 2: CREATE KEYPAIR AND SECURITY GROUP RULE

1. If do not have keypair in ~/.ssh run command:
   ssh-keygen -q -N ""

2. Add keypair to openstack:
   openstack keypair create --public-key ~/.ssh/id_rsa.pub mykey

3. Verify new keypair has been added:
   openstack keypair list

4. Add security group rule for ICMP and SSH
   openstack security group rule create --proto icmp default
   openstack security group rule create --proto tcp --dst-port 22 default

5. Verify security group has been added.
   openstack security group rule list

STEP 3: CREATE A VM INSTANCE

6. To create the VM we will need to gather information. Run the following commands to get flavor, image, and network-id:
   openstack flavor list
   openstack image list
   openstack network list

7. Run command to create VM:
   openstack server create --flavor m1.nano --image cirros --nic net-id=<PROVIDER NETWORK ID> --security-group default --key-name mykey cirros1

STEP 4: VERIFICATION

8. Verify VM has been created and get IP address for VM.
   openstack server list
9. Log into your new instance via SSH.

STEP 5: DELIVERABLES

10. As a group present the following to the TA or Instructor. It can be a video presentation submitted in canvas or in person.
    a. Logging into new instance using ssh keys.
    b. Output of the following commands:
       i. **openstack server create…**
       ii. **openstack server list**
       iii. **openstack keypair list**
       iv. **openstack security group rule list**
       v. **openstack flavor list**
       vi. **openstack image list**
       vii. **openstack network list**

SETTING UP PYTHON ENVIRONMENT

If running on another computer besides the controller you will need to setup the Python environment. Unless specified the commands are the same on Linux or Windows.

CREATE VIRTUAL ENVIRONMENT

```
mkdir virt_env
cd virt_env
python -m venv openstack
```

ACTIVATE VIRTUAL ENVIRONMENT

```
openstack\bin\activate
```

INSTALL PACKAGES

```
pip install -U pip
pip install -U setuptools
pip install python-openstackclient
```