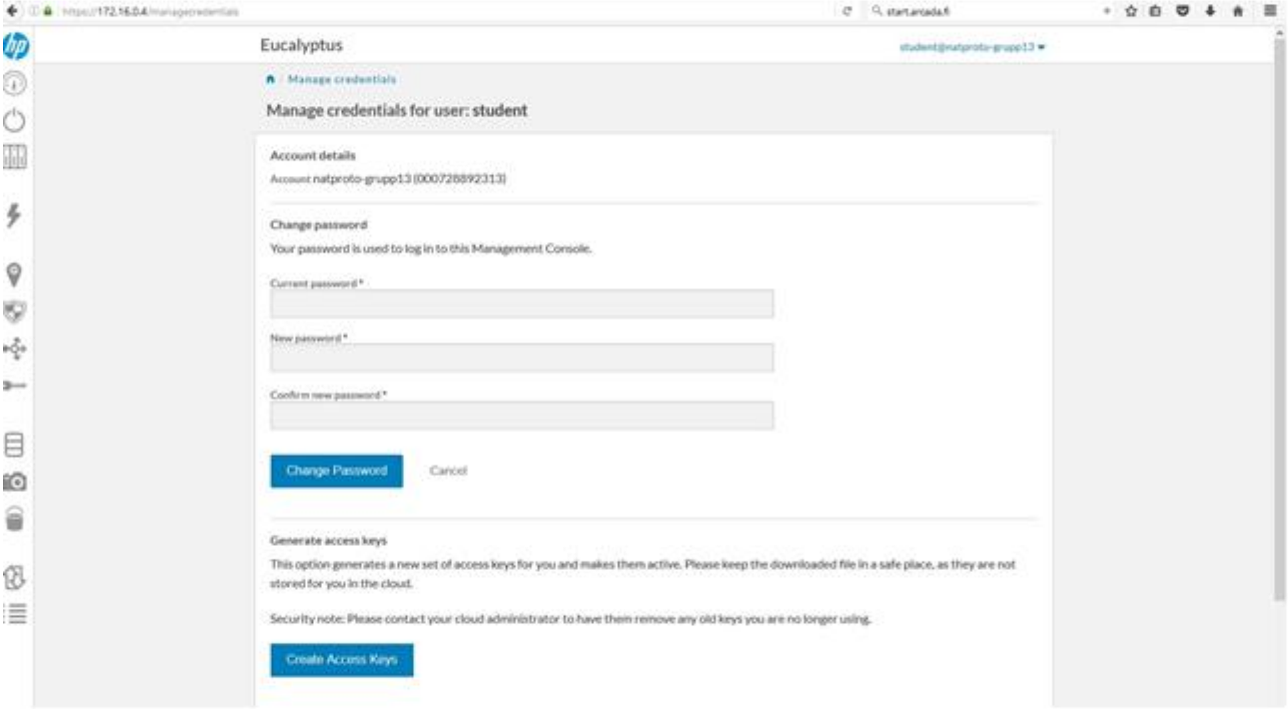
Contents

1. Read on your own chapter 3.3

2. login to Arcadas Eucalyptus cloude controller:

By openning a browser and browse to http://172.16.0.4
Then we chose as Account Name: NightProtector Group13, username: student and password: natproto17

3. Change the password for the (your) group as shown below:



Manage credentials for user: student

Account details

Account natproto-grupp13 (000728892313)

Change password

Your password is used to log in to this Management Console.

Current password *

New password *

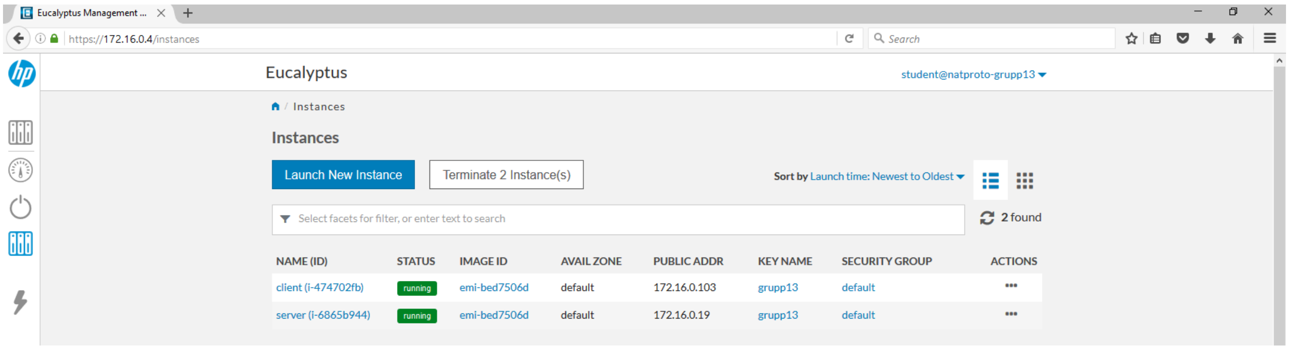
Confirm new password *

Generate access keys

This option generates a new set of access keys for you and makes them active. Please keep the downloaded file in a safe place, as they are not stored for you in the cloud.

Security note: Please contact your cloud administrator to have them remove any old keys you are no longer using.

4. Create a new instance by lick launch new instance.

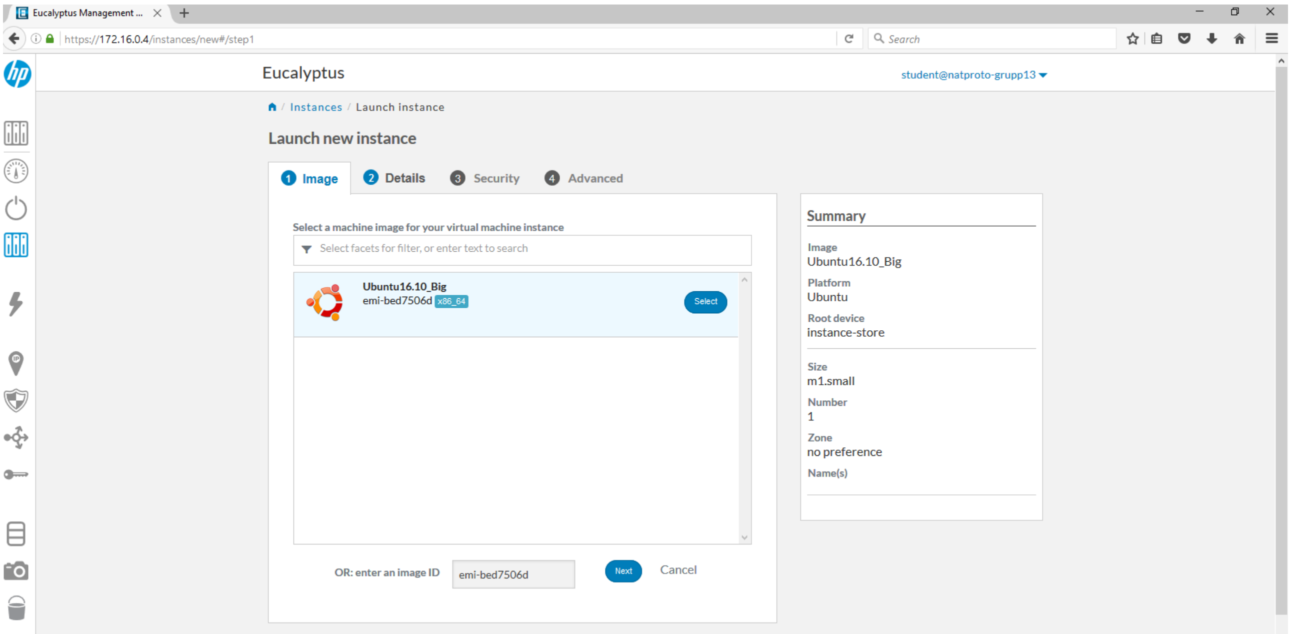


Eucalyptus Management ...
https://172.16.0.4/instances
Search
Eucalyptus
student@natproto-grupp13
Instances
Launch New Instance
Terminate 2 Instance(s)
Sort by Launch time: Newest to Oldest
Select facets for filter, or enter text to search
2 found

Instances

NAME (ID)	STATUS	IMAGE ID	AVAIL ZONE	PUBLIC ADDR	KEY NAME	SECURITY GROUP	ACTIONS
client (i-474702fb)	running	emi-bed7506d	default	172.16.0.103	grupp13	default	•••
server (i-6865b944)	running	emi-bed7506d	default	172.16.0.19	grupp13	default	•••

Select "Ubuntu16.10_Big



Eucalyptus Management ...
https://172.16.0.4/instances/new#/step1
Search
Eucalyptus
student@natproto-grupp13
Instances / Launch instance
1 Image
2 Details
3 Security
4 Advanced
Select facets for filter, or enter text to search
Select
Next
Cancel

Launch new instance

Select a machine image for your virtual machine instance

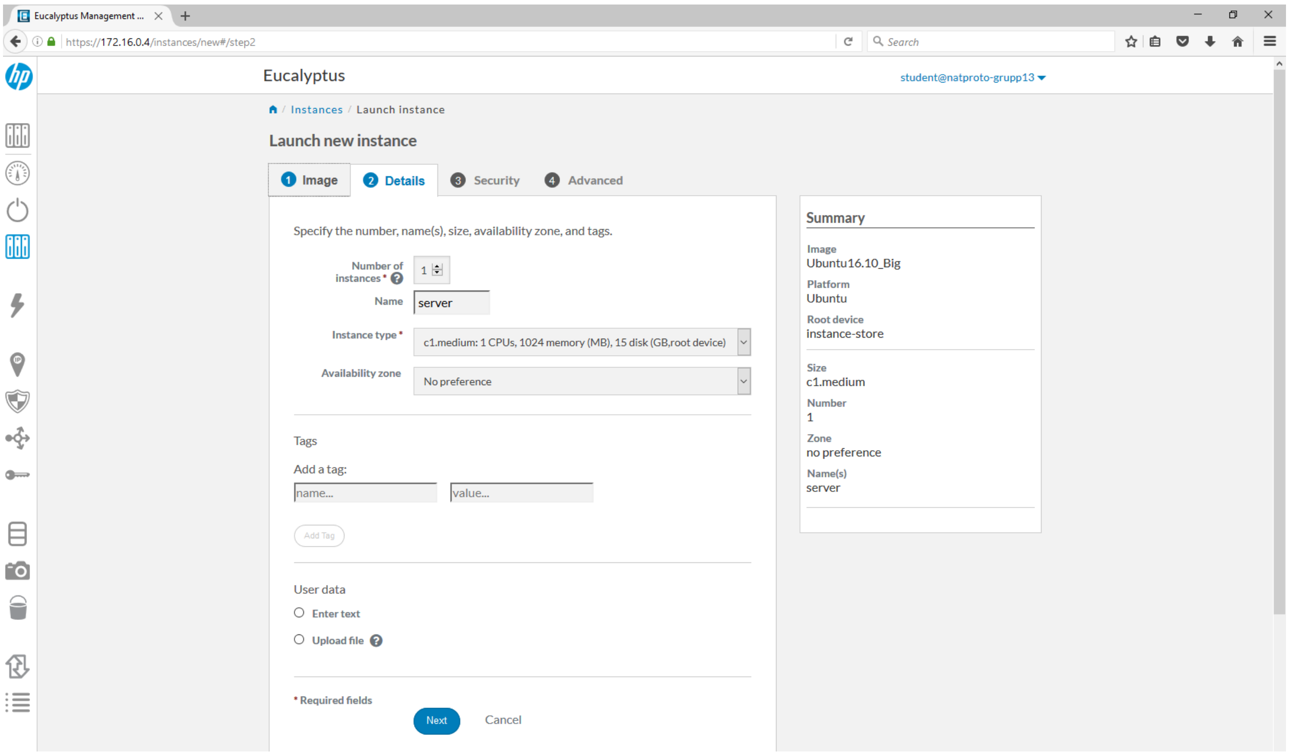
Ubuntu16.10_Big
emi-bed7506d x86_64

OR: enter an image ID: emi-bed7506d

Summary

Image: Ubuntu16.10_Big
Platform: Ubuntu
Root device: instance-store
Size: m1.small
Number: 1
Zone: no preference
Name(s)

Choose the name as “ Server ”
Selected "c1.medium" as "instance type"
Create a new key pair for SSH login



Launch new instance

Specify the number, name(s), size, availability zone, and tags.

Number of instances *: 1
Name: server
Instance type *: c1.medium: 1 CPUs, 1024 memory (MB), 15 disk (GB,root device)
Availability zone: No preference

Tags

Add a tag:

User data

○ Enter text

○ Upload file

* Required fields

Summary

Image: Ubuntu16.10_Big
Platform: Ubuntu
Root device: instance-store
Size: c1.medium
Number: 1
Zone: no preference
Name(s): server

5. Configuring the firewall for the new instance to approve incoming SSH traffic:

Make a copy of the default SSH configuration and rename it as factory default.

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.factory-defaults
```

After the backup has been made, you'll need to modify its permissions.

```
sudo chmod a-w /etc/ssh/sshd_config.factory-defaults

sudo gedit /etc/ssh/sshd_config
```

Restart ssh service with the following command:

```
systemctl restart ssh

or
service ssh restart
```

6. Log on to your instance with SSH

```
ssh -i grupp13.pem ubuntu@172.16.0.19
```

7. Configuring the SSH server on the instance:

The config file is in: ‘/etc/ssh/sshd_config

Turn on password authentication with:

PasswordAuthentication yes

8. How SSH works? How does the login happen and how the communication gets encrypted?

It is a secure (network) protocol which is used to remotely and securely connect and administer servers with the help of several encryption technologies. In other words, it provides secure communications between 2 systems applying a server/client architecture and users are allowed to remotely log into server host systems.

Instead of using a password, you can login with public key-private key pairs.

With a client-server model you will be able to implemented SSH connection

Password logins are encrypted and are easy to understand for new users.

One can log on different servers without needing different passwords. Authentication can be done via the personal private key on all servers.

Password authentication is easier to guess the public-private key due to less randomness. Using RSA/DSA keys can also provide 2 factors - what one has (private key) and what one know (passphrase). If subjected to a Man-In-The-Middle attack a password would be compromised, with password auth, while only access to the host on the other side of the MITM attack would be compromised when using pub-private key.

Authentication

Once the secure connection is established between the client and the server, the client has to log on to the server to obtain an access right. There are several methods:

- the most well-known method is the traditional password. The client sends a login and a password to the server via the secure connection and the server checks whether the user in question has access to the machine and whether the password provided is valid.
- a lesser known but more flexible method is the use of public keys. If the client chooses key authentication, the server will create a *challenge* and give access to the client if the latter is able to decrypt the challenge with its private key