



Installing and Scaling out Ubuntu Enterprise Cloud in Virtual Environment

Supplement to

“Guidelines for Building a Private Cloud
Infrastructure”

Zoran Pantić and Muhammad Ali Babar

Tech Report TR-2012-154

ISBN: 978-87-7949-255-4

IT University of Copenhagen, Denmark, 2012

Summary

This document contains the supplemental material to the book “Guidelines for Building a Private Cloud Infrastructure”. This document provides guidance on how to install Ubuntu Enterprise Cloud in virtual environment, and afterwards how to scale out when needed.

The purpose of this supplemental book is to provide a practical, step-by-step, detailed guide on how to dimension and install the machines and network. Some initial steps of configuring the cloud are also covered. The installation is performed in a virtual environment based on Windows 7 and VMware Workstation 7.

The cloud installation is performed using the (for the time being) newest version of the UEC, based on the Ubuntu 11.04. The installation is performed using “CD Install” method¹ (otherwise, there is also a “Package Install” method²). Eucalyptus version installed is 2.0.2. This document also includes the initial setup of the newly installed cloud, both using the command line tools, and GUI based tool HybridFox.

¹ <https://help.ubuntu.com/community/UEC/CDInstall>

² <https://help.ubuntu.com/community/UEC/PackageInstall>

Contents

Summary.....	1
Installation of the cloud.....	3
Machine configuration – initial setup.....	3
Network configuration	4
Installation of the servers.....	4
Installation of the first server (CLC, WS3).....	5
Installation of second server (CC, SC).....	34
Installation of third server (NC)	38
Verifying the cloud installation.....	40
Running the cloud.....	41
Cloud web interface	41
Initial steps	44
Scaling out the cloud – adding NC to a cluster	52
Installation of fourth server (NC).....	52
Scaling out the cloud – adding a whole cluster	55
Installation of fifth server (CC, SC).....	55
Installation of sixth server (NC)	58
Verifying the cloud after the scale-out.....	60

Installation of the cloud

The characteristics of the host system (HP Z600 Workstation) are as follows:

- 2 x Intel Xeon E5530 CPU 2.4GHz
- 12 GB DDR3 RAM
- 840 GB hard disk (3 spindles in RAID 0 configuration on Intel ICH8R SATA RAID controller)
- Windows 7 OS x64
- VMware Workstation 7

The cloud installation described here is performed using the (for the time being) newest version of the UEC, based on the Ubuntu 11.04 ("ubuntu-11.04-server-amd64.iso" CD image). To get the most of the physical server, we choose the 64-bit architecture, although a 32-bit version is also available, if implementing on the older, x86 based architectures.

A "long-term support" (LTS) release is also available (10.04) if more stability needed, or for larger deployments.

Machine configuration – initial setup

Initial setup is performed on 3 servers – first server being cloud front end, second server being responsible for the cluster, and the third server being the compute node.

Here is how the servers should be configured:

UECserver01

Roles: CLC, WS3

Processor architecture: 64 bit

VT: not necessarily VT enabled

Network: public (VMnet0), private (VMnet2)

Memory	2048 MB
Processors	1
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using drive D:
Network Adapter	Bridged
Network Adapter 2	Custom (VMnet2)
Display	Auto detect

UECserver02

Roles: CC, SC

Processor architecture: 64 bit

VT: not necessarily VT enabled

Network: public (VMnet0), private (VMnet2)

Memory	2048 MB
Processors	1
Hard Disk (SCSI)	400 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Bridged
Network Adapter 2	Custom (VMnet2)
Display	Auto detect

UECserver03

Roles: NC

Processor architecture: 64 bit

VT: VT enabled

Network: private (VMnet2)

Memory	4096 MB
Processors	2
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using drive D:
Network Adapter	Custom (VMnet2)
Display	Auto detect

Here is the overview in a table:

Server name	Server role	Processors	RAM (GB)	Hard disk (GB)	Eth0	Eth1
UECserver01	CLC, WS3	1	2	200	VMnet0	VMnet2
UECserver02	CC, SC	1	2	400	VMnet0	VMnet2
UECserver03	NC	2	4	200	VMnet2	-

Network configuration

All networks run on a class \C private network range (subnet mask 255.255.255.0).

The networking in our setup is implemented with two networks – private and public. The public network would be accessible to users and administrators from the “outside world”, and the private network is reserved for the backend communication, and is private for the cloud.

Here is the overview in a table:

Name	VMware name	Network	Subnet mask	Gateway	DNS1	DNS2
Public	VMnet0	192.168.1.0	255.255.255.0	192.168.1.1	193.162.153.164	194.239.134.83
Private	VMnet2	10.0.0.0	255.255.255.0	10.0.0.1	10.0.0.1	-

Managed-NOVLAN networking mode is chosen, since it gives a variation of possibilities close to the ones that would be needed in production environments. NOVLAN is chosen simply for the reason that no VLAN network components are available in the virtual environment. For more details on the 4 networking modes in UEC, please refer to the main document.

The public DNS servers are very connection specific, and should be obtained and configured in collaboration with you internet service provider, or internal IT department.

IP addresses allocated for the cloud instances as public IP addresses: 192.168.1.100 - 192.168.1.254 (divided between clusters, if several clusters present).

Installation of the servers

For more details on installation of UEC, please refer to Ubuntu Documentation³.

Installation is performed from “ubuntu-11.04-server-amd64.iso” installation CD.

The installation could be divided in two parts: first part is a usual Ubuntu server installation, and second part is related to installing of cloud components.

The screen shots with comments and explanations are given for the whole process of installing the first server.

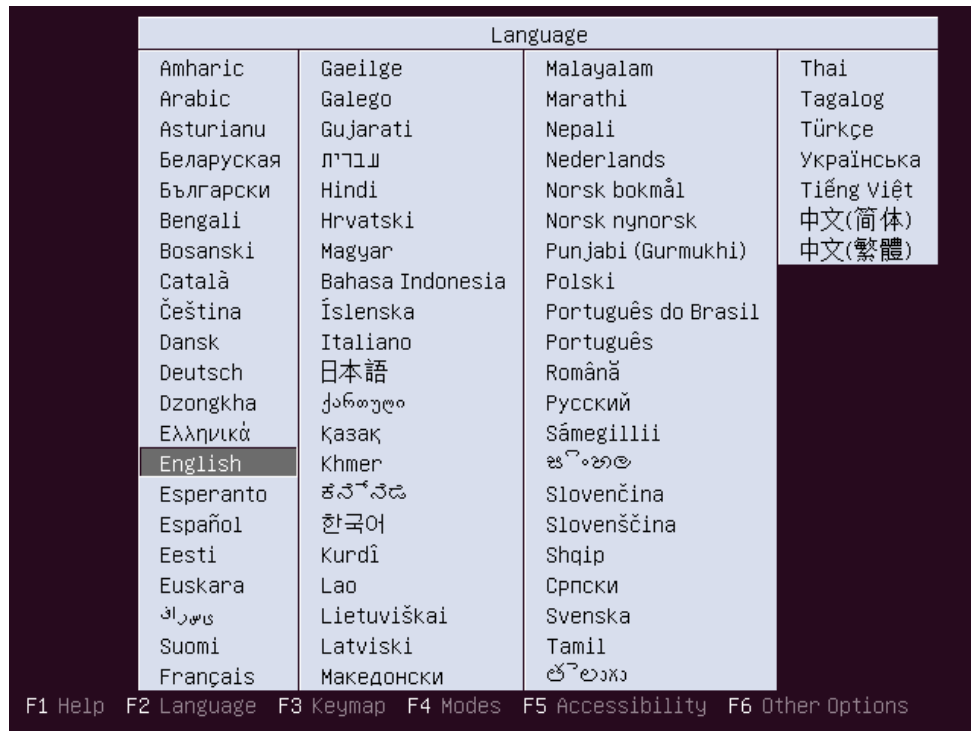
Installing later servers, there are screenshots only for the parts pertaining to the installation and configuration steps that are different from the installation of the previous server(s).

³ <https://help.ubuntu.com/community/UEC>

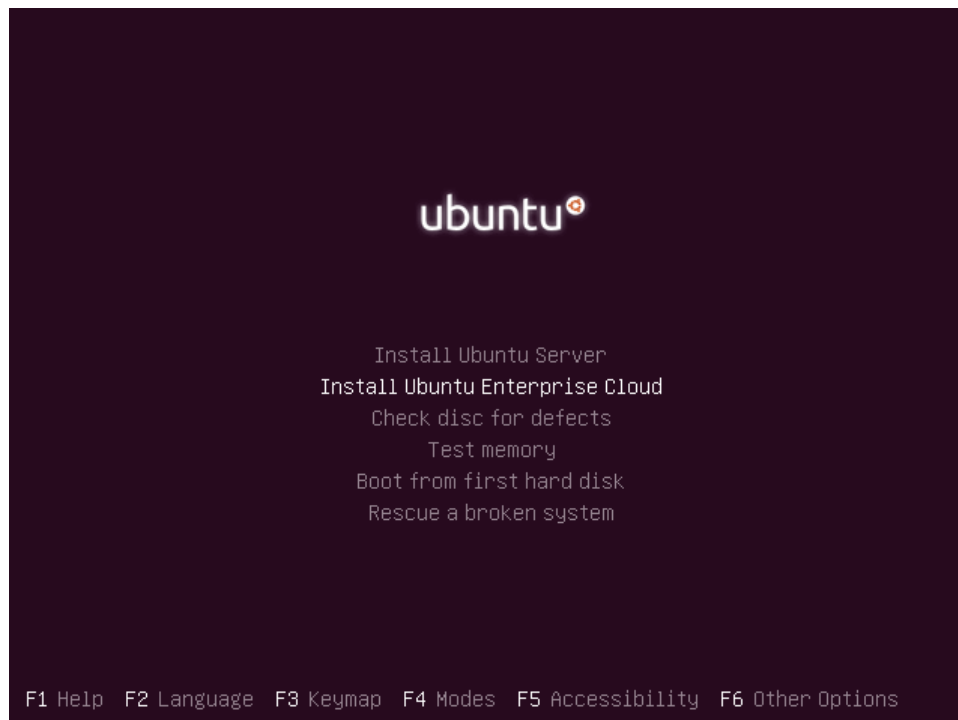
Installation of the first server (CLC, WS3)

Mount the installation media, and boot from it.

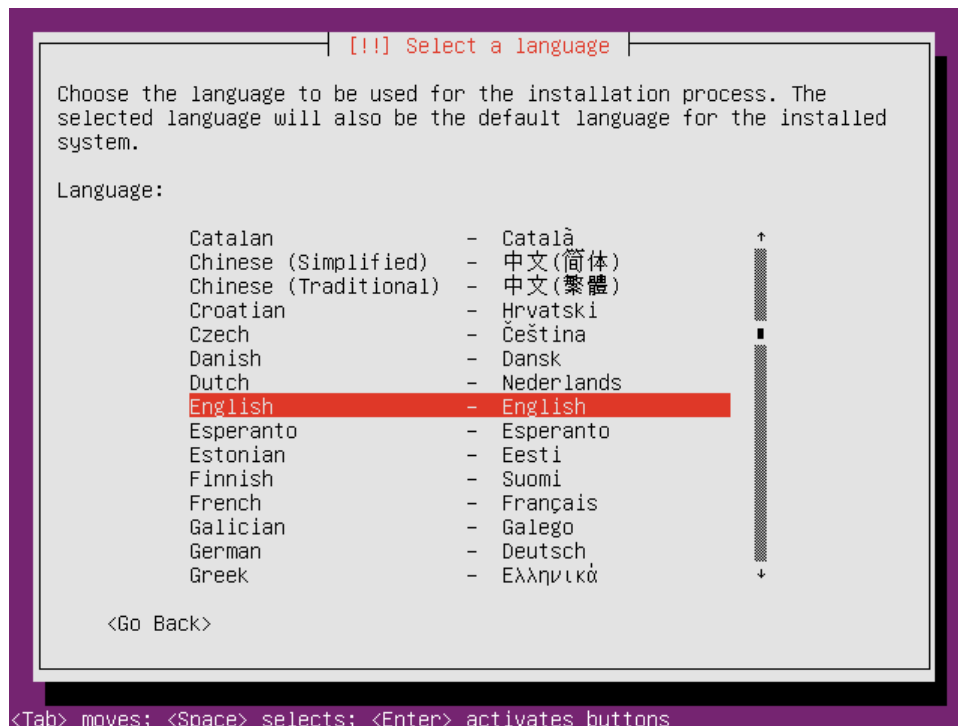
Choose the language – English.



Choose “Install Ubuntu Enterprise Cloud”.



Choose English as installation language, and the default language for the installed system.



Select your location – other:



Select your location – Europe:

[[!]] Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

Select the continent or region to which your location belongs.

Continent or region:

Africa

Antarctica

Asia

Atlantic Ocean

Caribbean

Central America

Europe

Indian Ocean

North America

Oceania

South America

other

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

Select your location – Denmark:

[[!]] Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

Listed are locations for: Europe. Use the <Go Back> option to select a different continent or region if your location is not listed.

Country, territory or area:

Bulgaria

Croatia

Cyprus

Czech Republic

Denmark

Estonia

Faroe Islands

Finland

France

Georgia

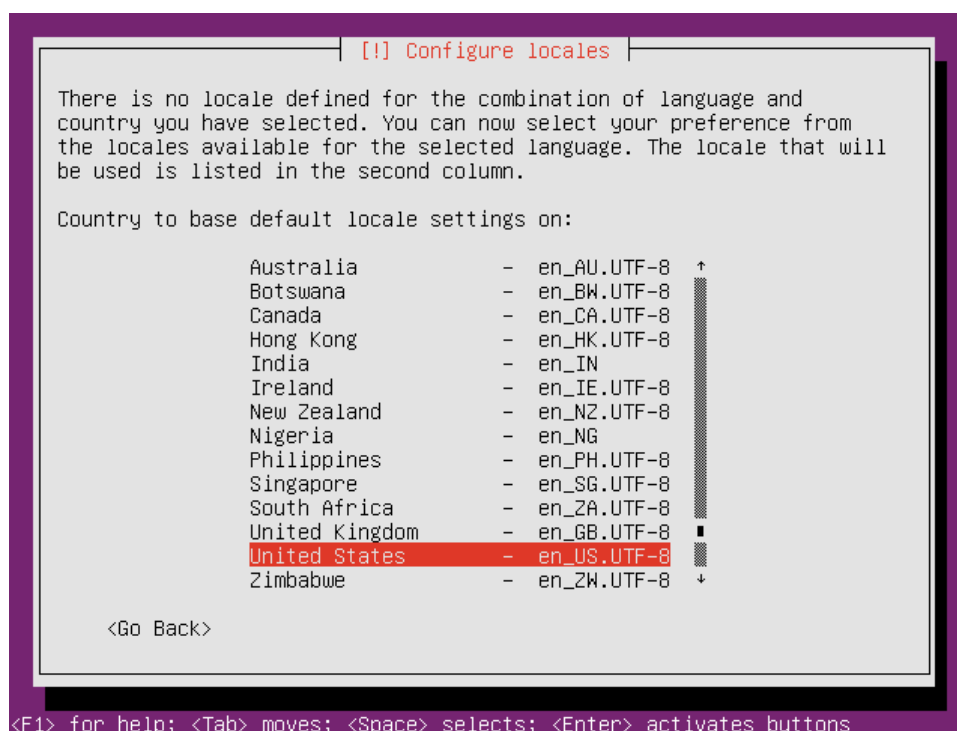
Germany

Gibraltar

<Go Back>

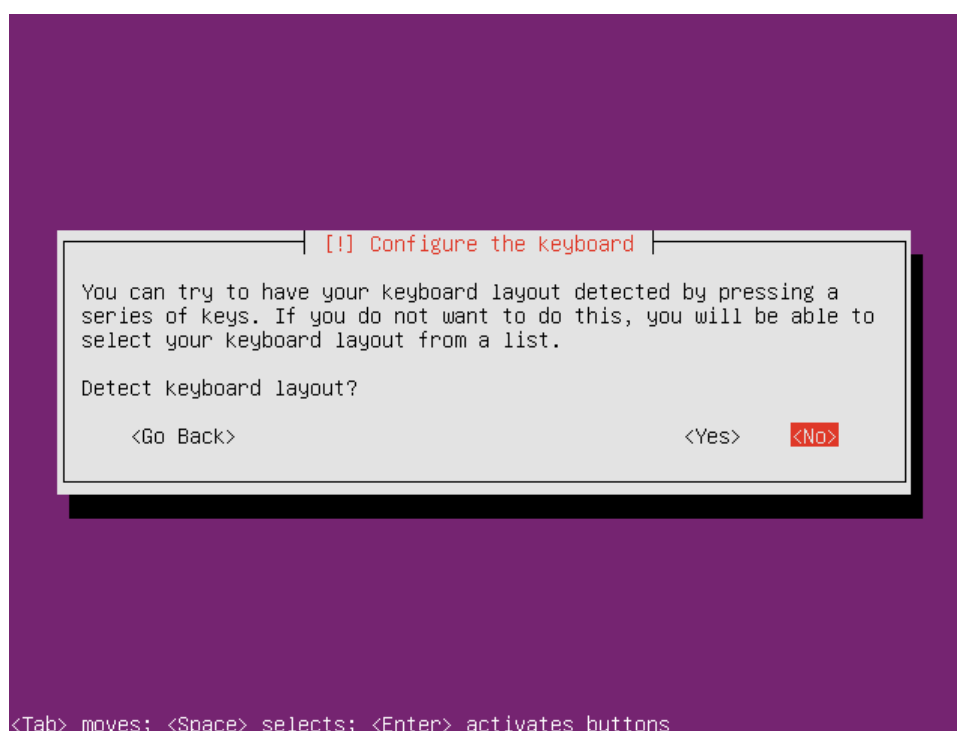
<Tab> moves; <Space> selects; <Enter> activates buttons

Configure locales – select United States:



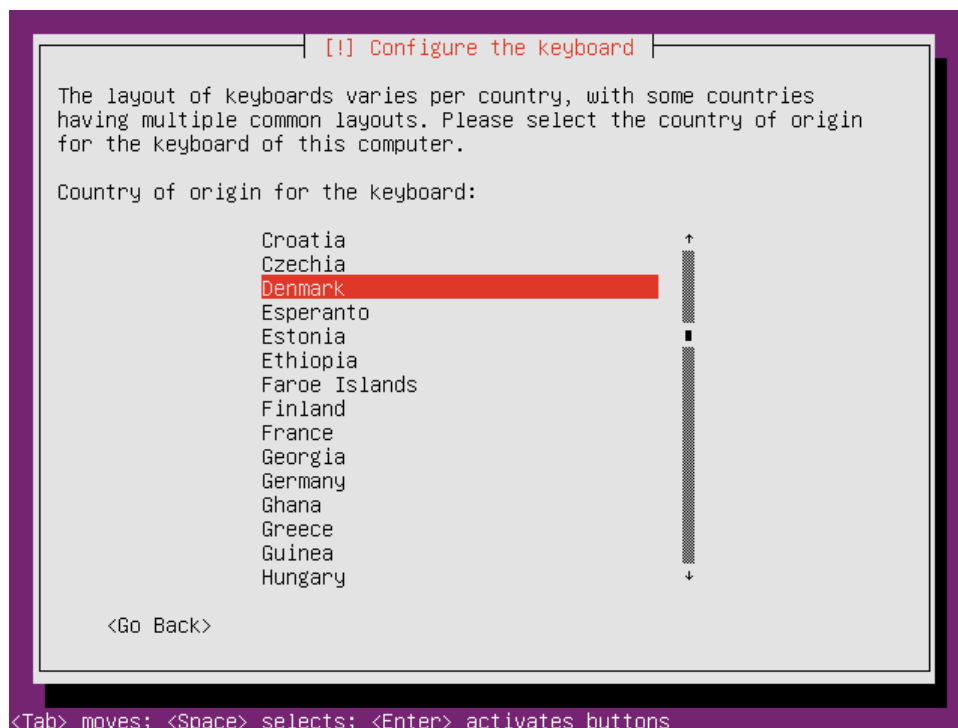
This comes only if no locale is defined for the combination of language and country of your selection. If we were choosing i.e. Portuguese and Brazil, everything would be fine, since Portuguese is defined for Brazil.

Configure your keyboard - choose no:

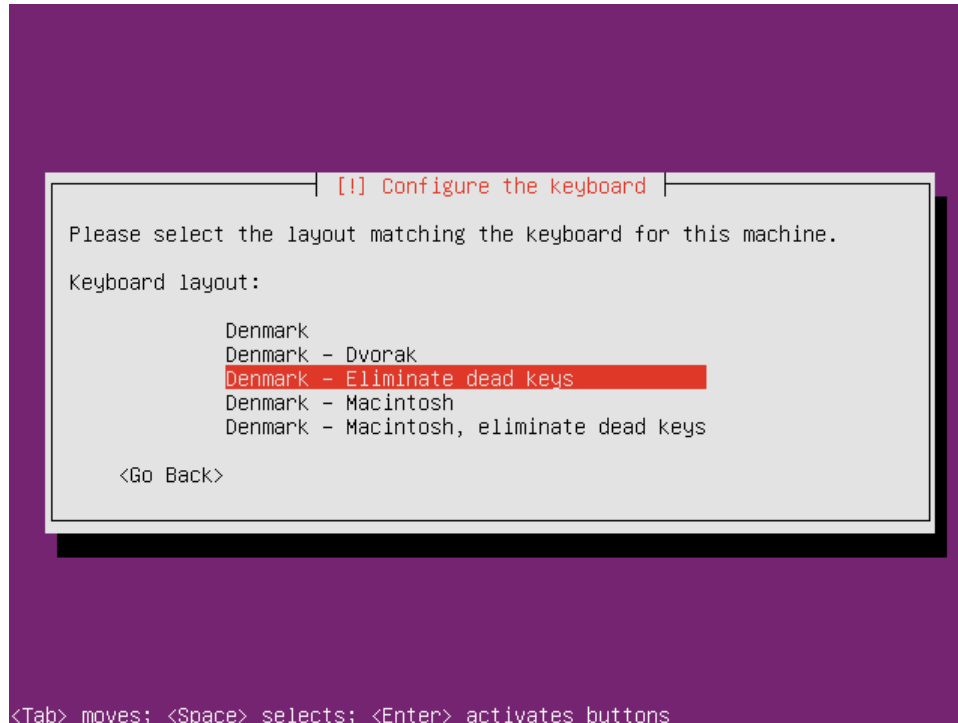


If you want your keyboard to be detected, you could choose yes and go through a wizard of options, ending with your keyboard identified.

Configure the keyboard for Denmark:

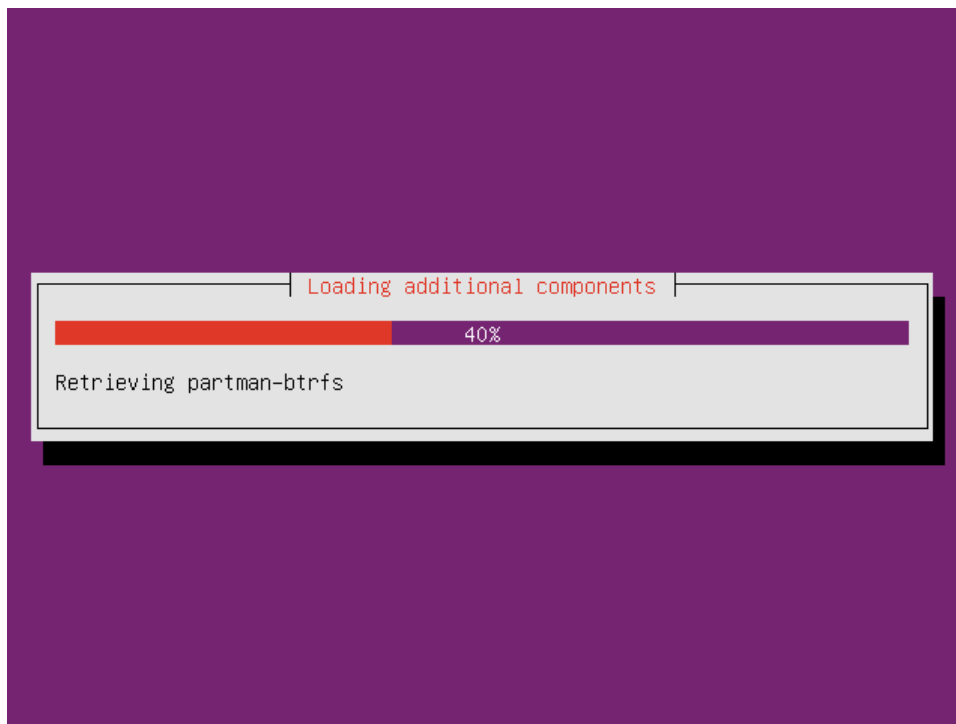


Choose Denmark – Eliminate dead keys:

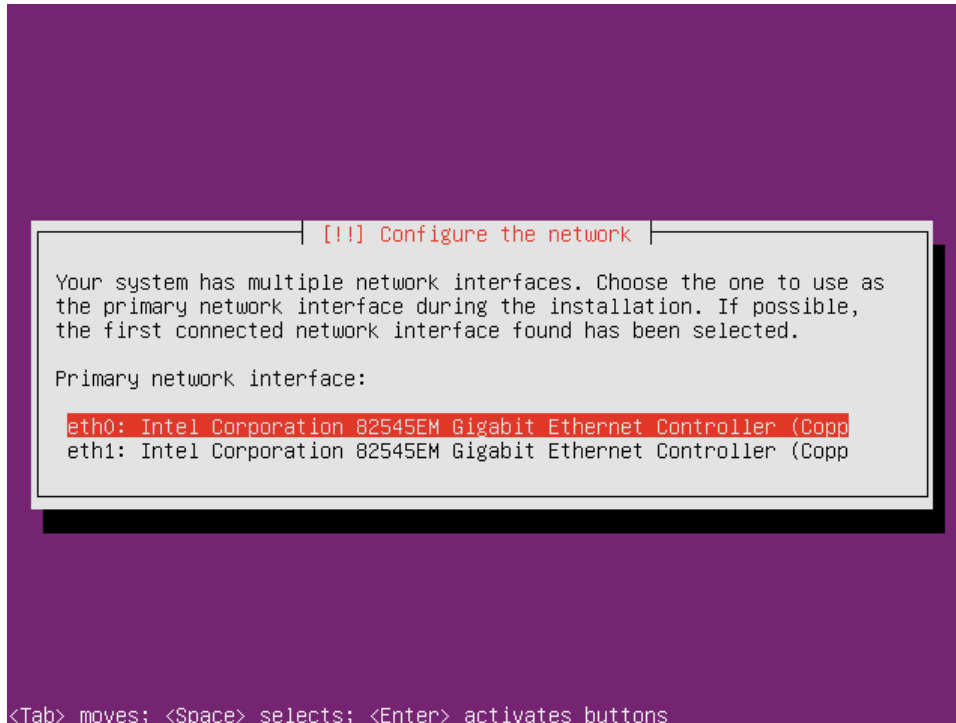


If you would get troubles with getting some special characters, like “~” and “|”, as a quick workaround you could make a SSH connection to the machine from a machine where you positively know that you can type those characters, and run the commands from there, instead from the local host.

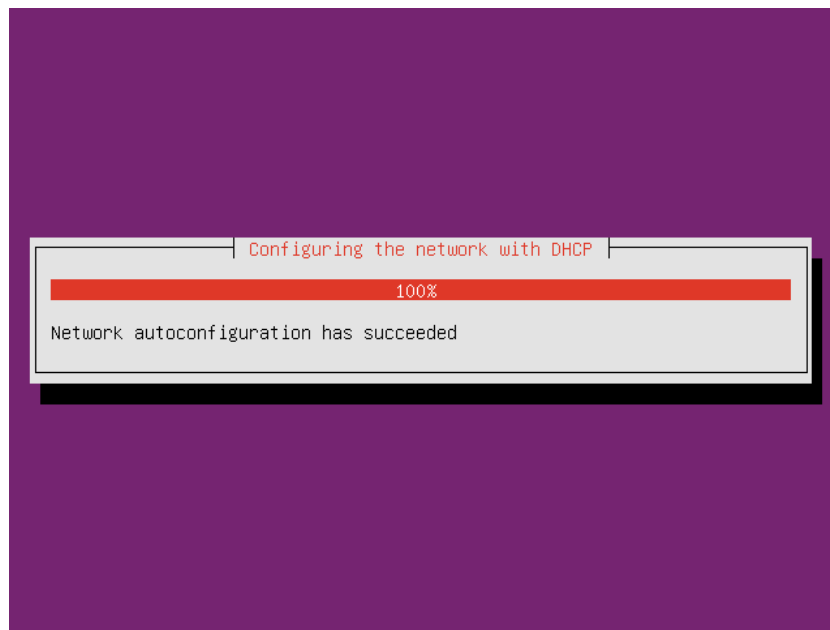
The installation starts loading additional components – this part should not take more than few minutes:



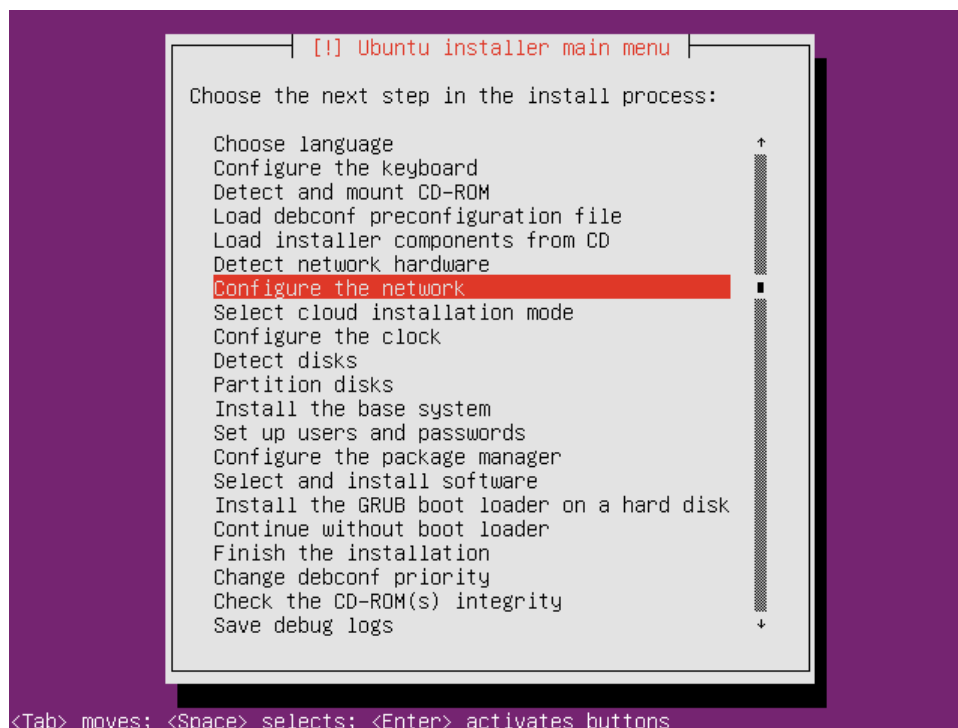
Next step is configuring network – choose the primary network interface for the installation:



The installation automatically configures this network interface for DHCP:



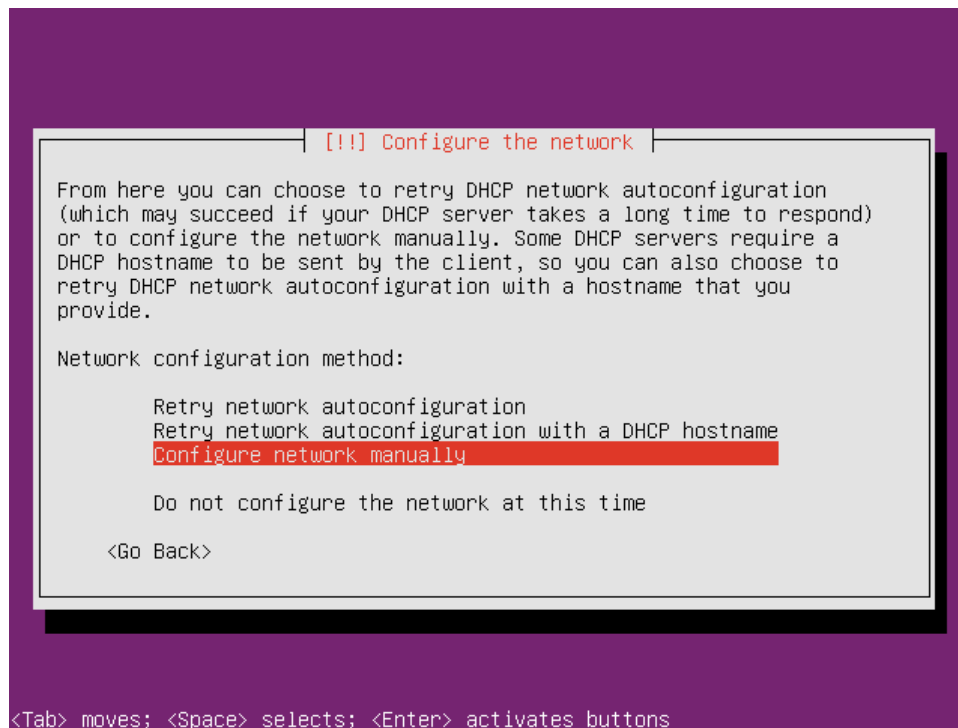
Since we want to assign static IP address for the network interface, be quick to press Enter (or Esc) just after previous option of choosing the network interface. But don't worry if you are not quick enough – pressing Esc later would just bring you to the following:



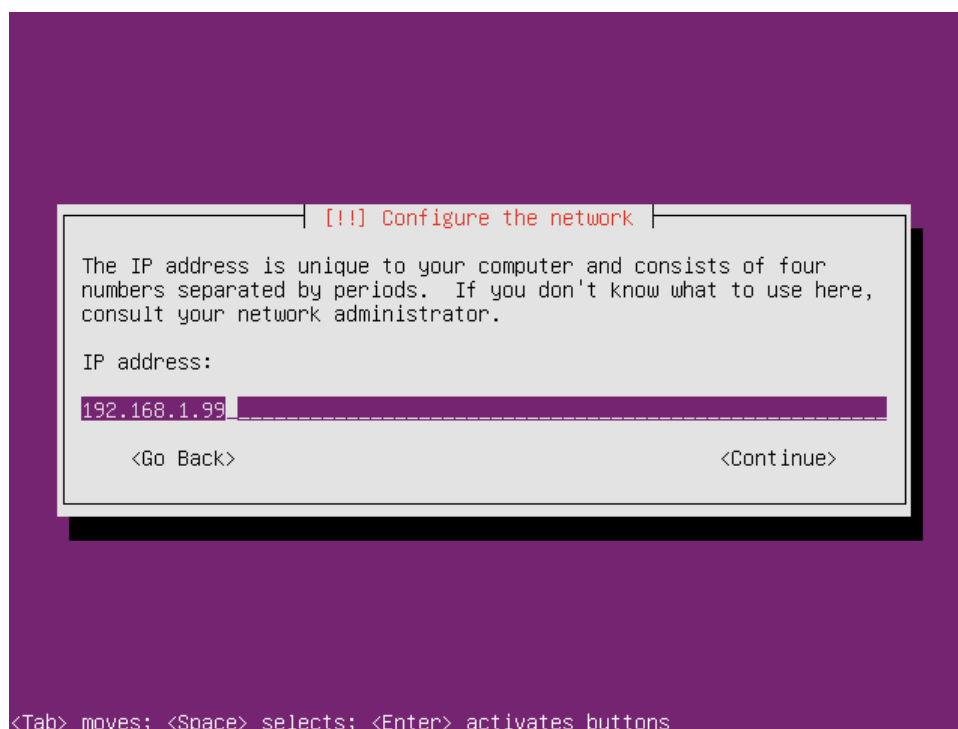
Just enter to the “Configure the network” again, and you will get the option of configuring static IP.

Also, pressing “Esc” during almost the whole process of installation would bring this main menu up.

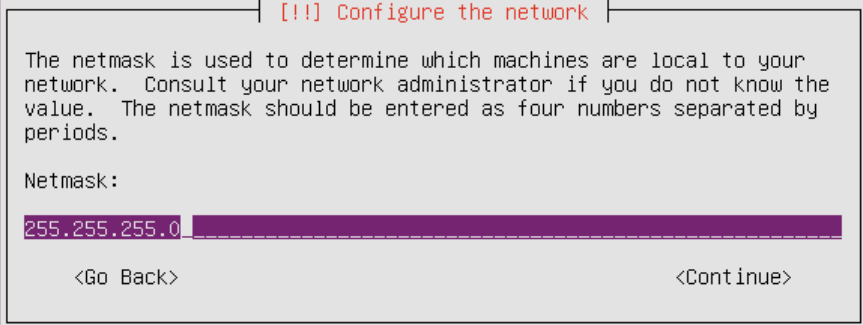
Multiple choices for configuring the network are presented, where one of the options would be configuring the network manually:



Put the machines IP address in:



Put the netmask for the class C networks in:



[!!] Configure the network

The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

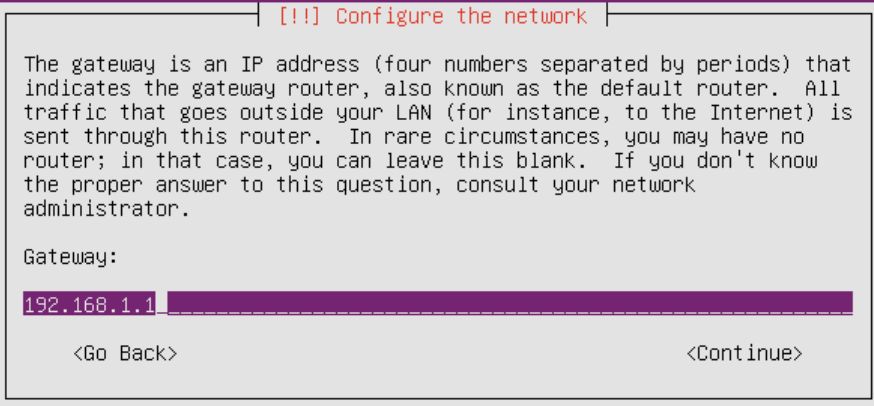
Netmask:

255.255.255.0

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Now the gateways IP address:



[!!] Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

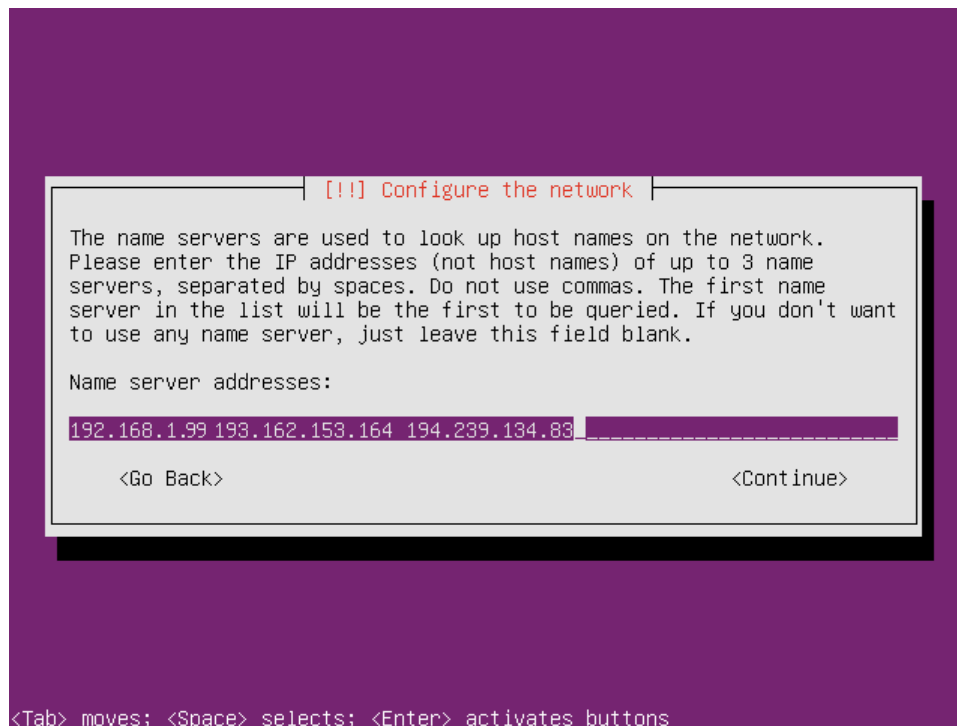
Gateway:

192.168.1.1

<Go Back> <Continue>

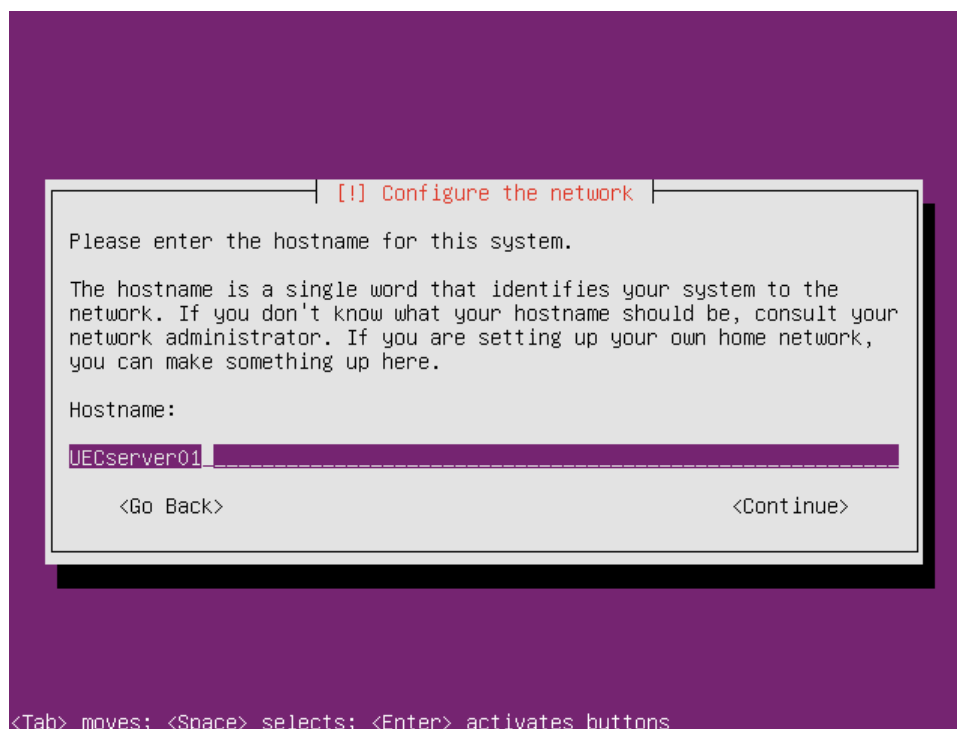
<Tab> moves; <Space> selects; <Enter> activates buttons

Put all the DNS servers that are available, separated by blank space:



The first one to be contacted would be the first one from the list. In our case it is the local server's address (192.168.1.99), since we will install DNS server on this server later on.

Choose the name for the host. Remember that hostnames are case sensitive in UNIX / Linux.



In our case, we choose to identify that the server is hosting UEC on it, but we don't designate the server role in the name, since server roles can be changed. Choosing "UECserverNN" would allow us to scale out to up to 100 hosts without getting into naming problems.

Domain name – since it is just a test implementation, we choose an "internal" name:

[!] Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

UECcloud.private

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

In the real implementation, we could choose the organization's domain name, which would normally be provided by the organization's IT department (such as i.e. "cloud.itu.dk").

For the initial install of the cloud, we just continue here, since there is no present Cloud Controller, and we are just installing one. If we were adding the server to an existing cloud, we would put the hostname or IP address of the Cloud Controller here (in case if it wasn't detected automatically, which it normally is).

[!] Select cloud installation mode

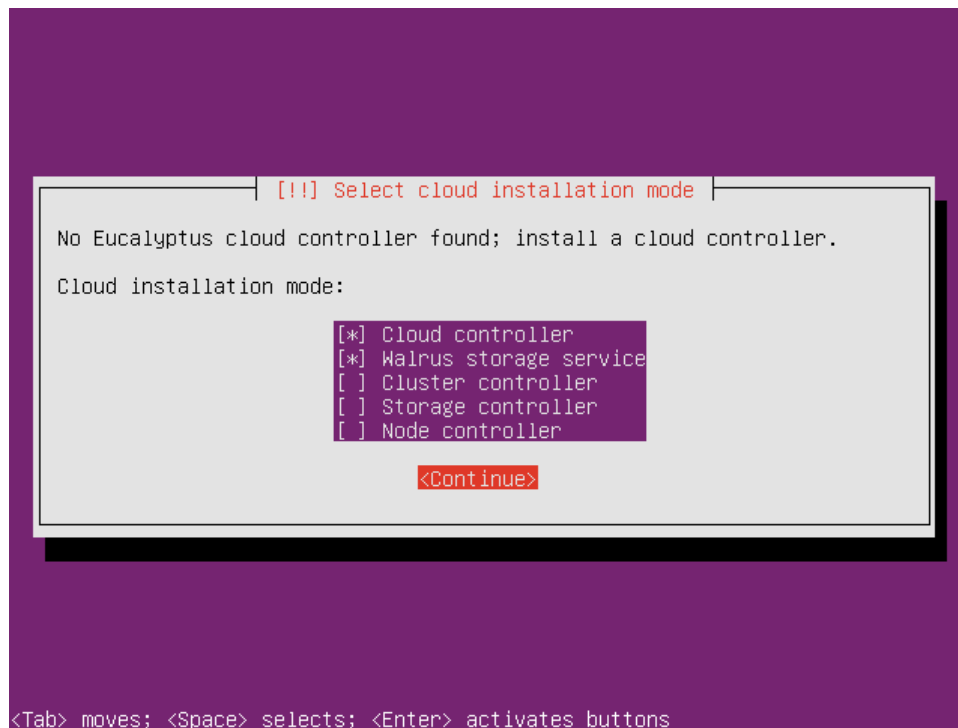
No Eucalyptus cloud controller was found on your network. If this is a mistake and there is in fact already a cloud controller, enter its hostname or IP address here. Otherwise, leave this blank.

Cloud controller address:

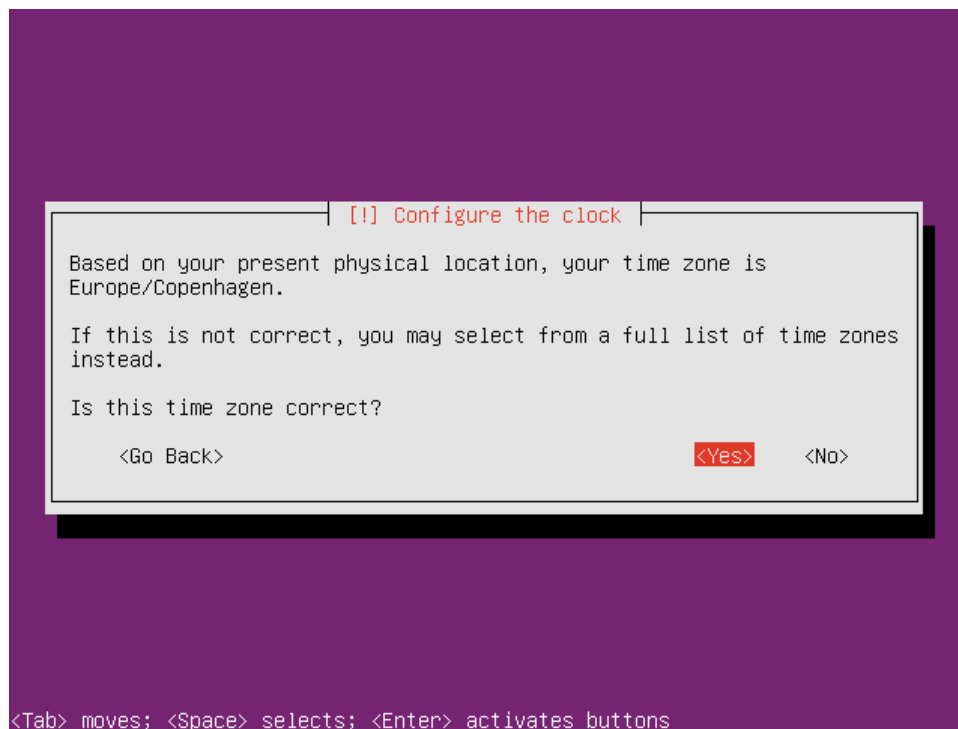
<Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Choosing the components to be installed on the first server – we install Cloud Controller and WS3. This is a design choice, since in our case we want to try scale out possibilities, and we are initially separating cloud and cluster components. We choose the components common for the whole cloud:

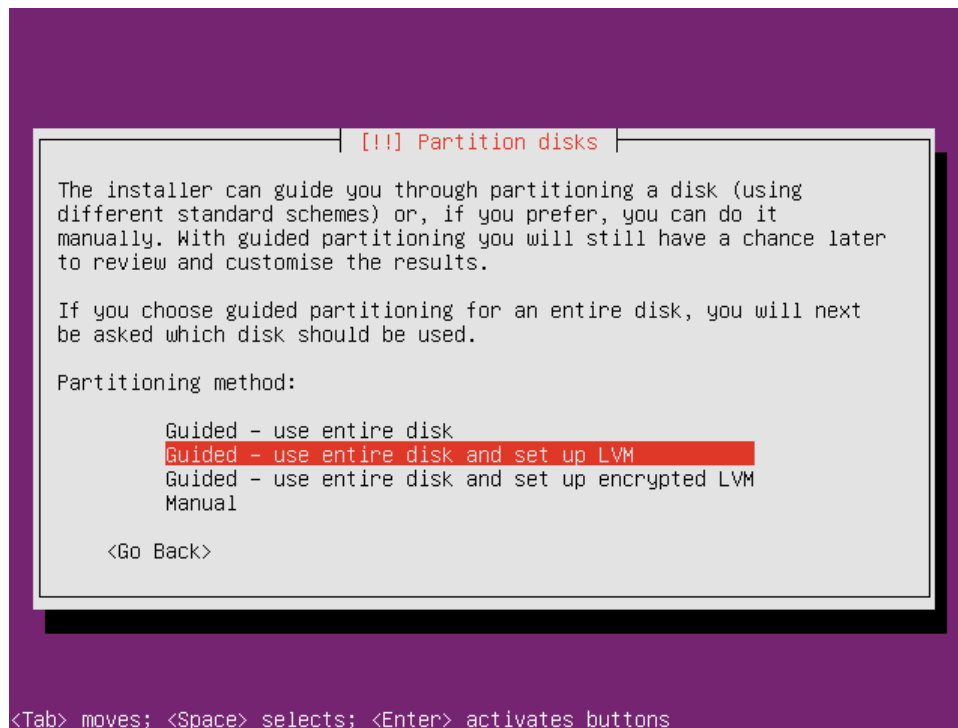


Confirm the time zone:



If not correctly detected, choose No, and you will get the choice of setting up the time zone.

Now we have a choice to partition our disk(s). For the sake of simplicity, choose a guided method, using the entire disk, and setting up LVM:



In our case, we have only one large disk, and we would just partition it using default options. If having several disks, we could choose another way of partitioning, for the sake of performance or redundancy.

Generally, for the local disk, RAID options should be configured on the controller level. That configuration is specific for each hardware supplier - please refer to the supplier's manuals. RAID 0 (stripping) would give us best performance and most space, but no redundancy. RAID 1 (mirroring) is having a bit better read performance than just one disk, but gives redundancy. RAID 5 is giving better performance and redundancy (for missing just one disk). The best option if having local disks would be RAID 10 (that is, mirroring of the two stripped volumes) giving us both performance of RAID 0 and redundancy of RAID 1, but then we have to have at least 4 disks.

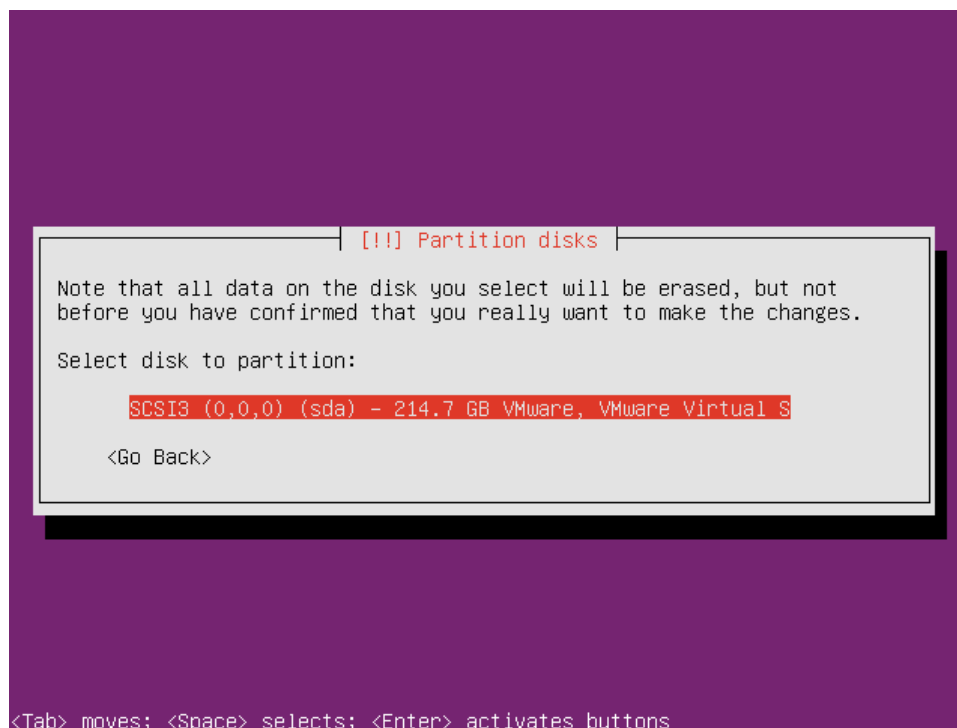
We could also choose to put the operating system on the local disks (in some RAID configuration, preferably RAID 1 and up) and put cloud specific storage on SAN (Storage Array Network), accessing it by either fiber net (optical, very quick but expensive) or iSCSI (using Ethernet infrastructure).

Logical Volume Manager (LVM), allows us to create logical volumes on physical hard disk(s). LVM volumes can be created on both software RAID partitions (that is, not having controller that supports RAID configuration, and doing it on the operating system level instead) and standard partitions residing on a single disk. Volumes can also be extended, giving greater flexibility to systems as requirements change. Choosing configuration using LVM has a greater degree of complication as side effect. Some of the terms used in the process are:

- Volume Group (VG): contains one or several Logical Volumes (LV);
- Logical Volume (LV): is similar to a partition in a non-LVM system; Multiple Physical Volumes (PV) can make up one LV, on top of which resides the actual EXT3, XFS, JFS, and other file system;
- Physical Volume (PV): physical hard disk or software RAID partition; the VG can be extended by adding more PVs.

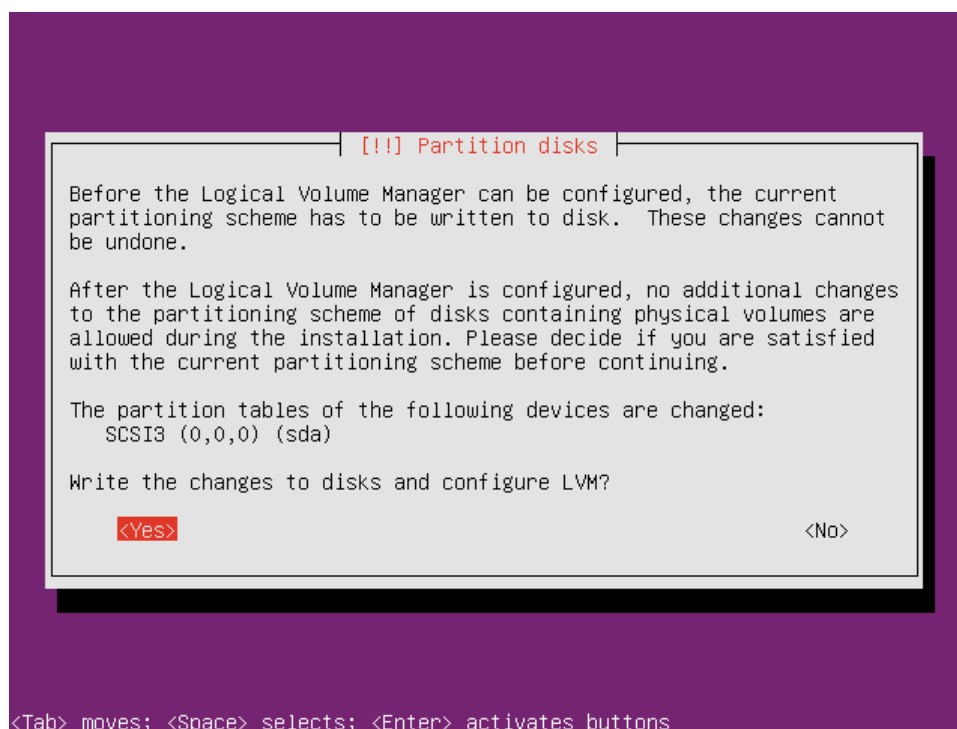
In our simple case, choosing LVM setup doesn't give any extra work. If having another disk configuration, choosing setup using LVM is ensuring that the configuration is done the right way in the terms of performance and redundancy, and is recommended.

In our case, we only have one disk to be partitioned:

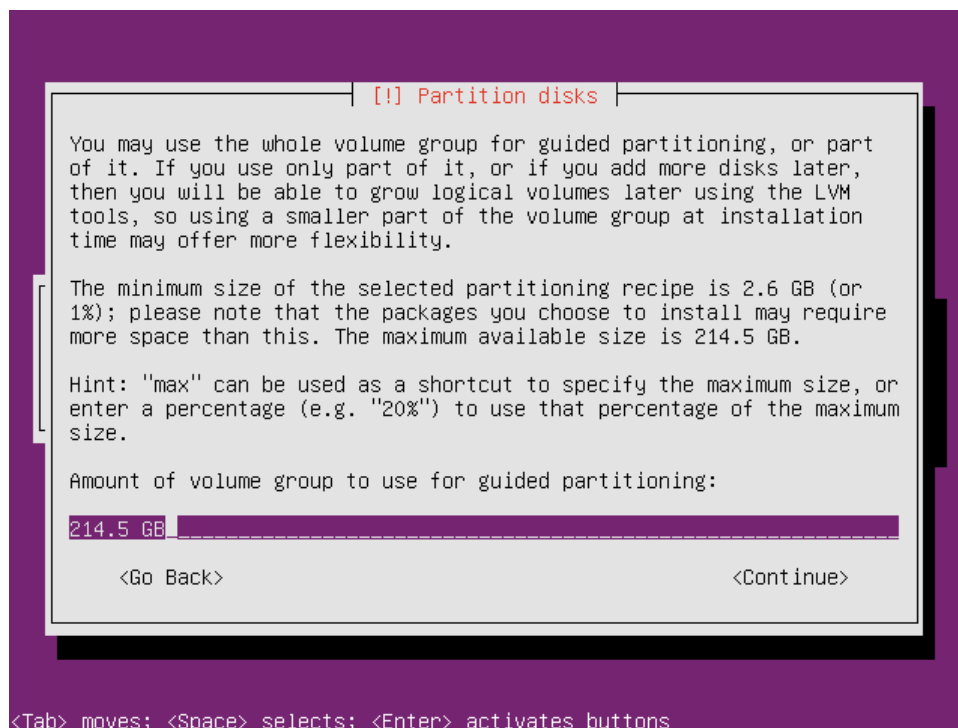


If the disk was used before, having some partitions on it, we would be prompted to overwrite the old configuration, warned that we would lose all the data saved on the disk.

Write the partition scheme to the disk:

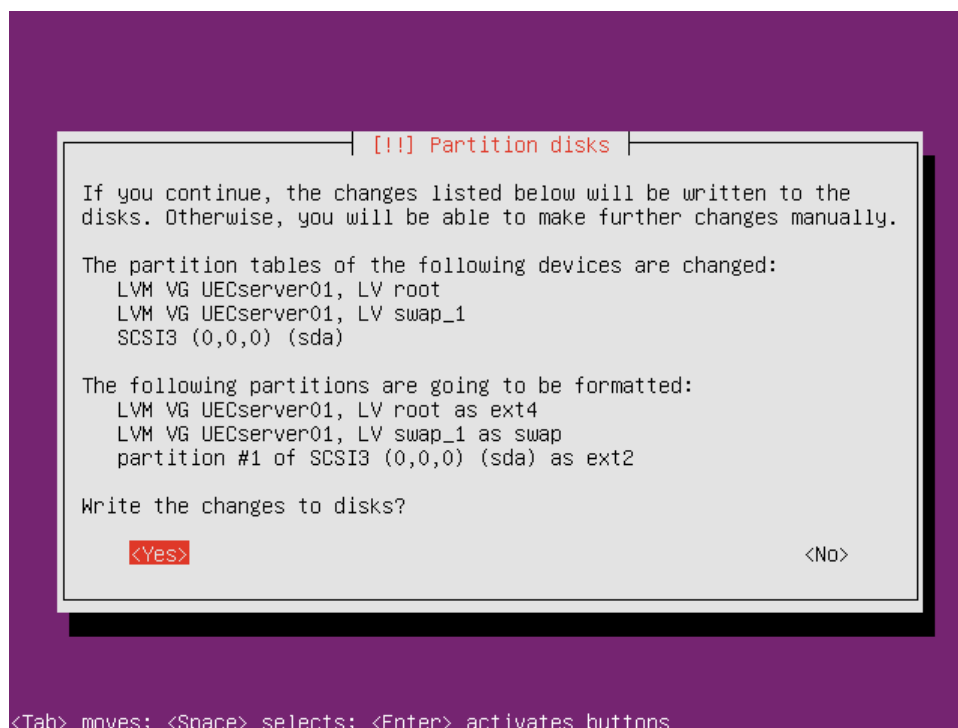


Choosing the amount of VG to use:



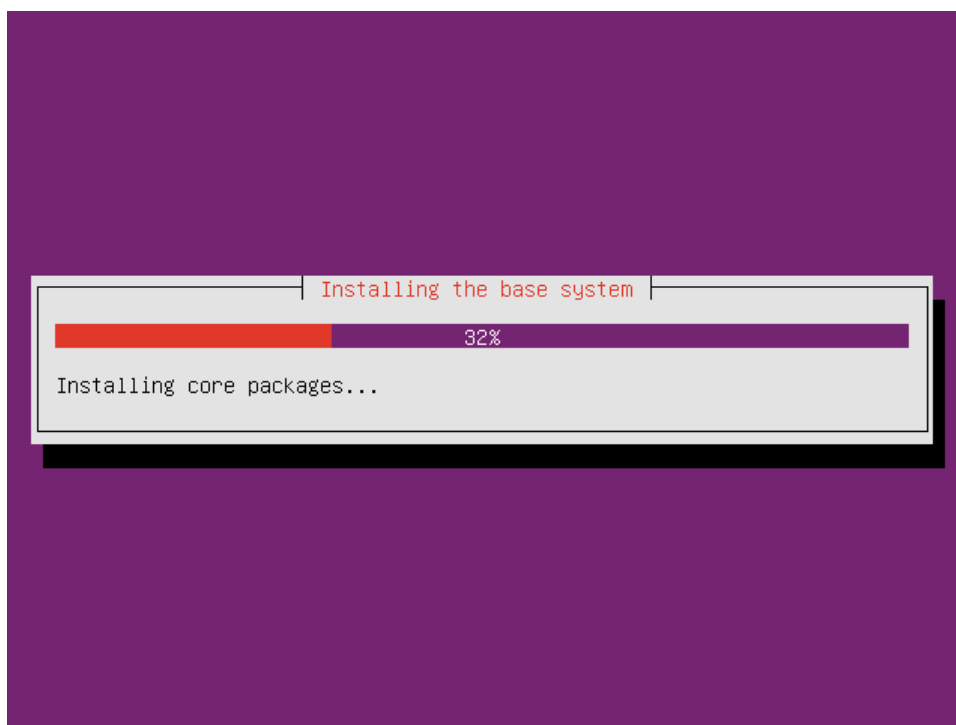
In our case, we use the whole disks capacity.

Writing the changes on the disk:



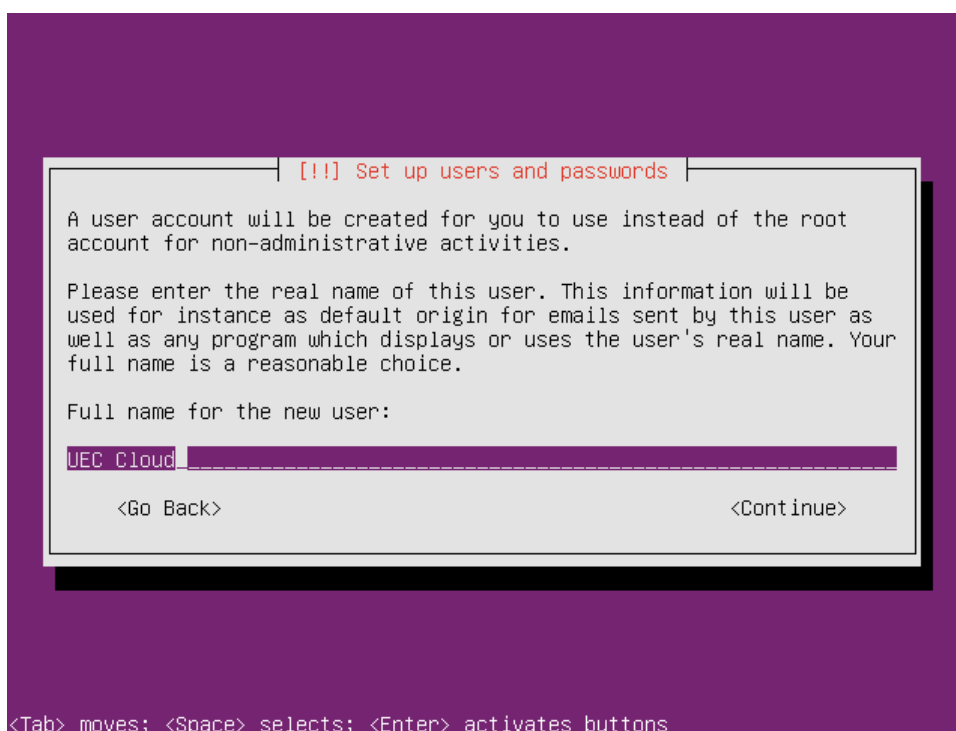
After the disk configuration, the base system installation starts. This could take from just a few minutes to tens of minutes, since the files are being copied from the installations media to the hard drive, and how

quick that would be done is depending on the speed of reading the installation media, and writing it on the disk.

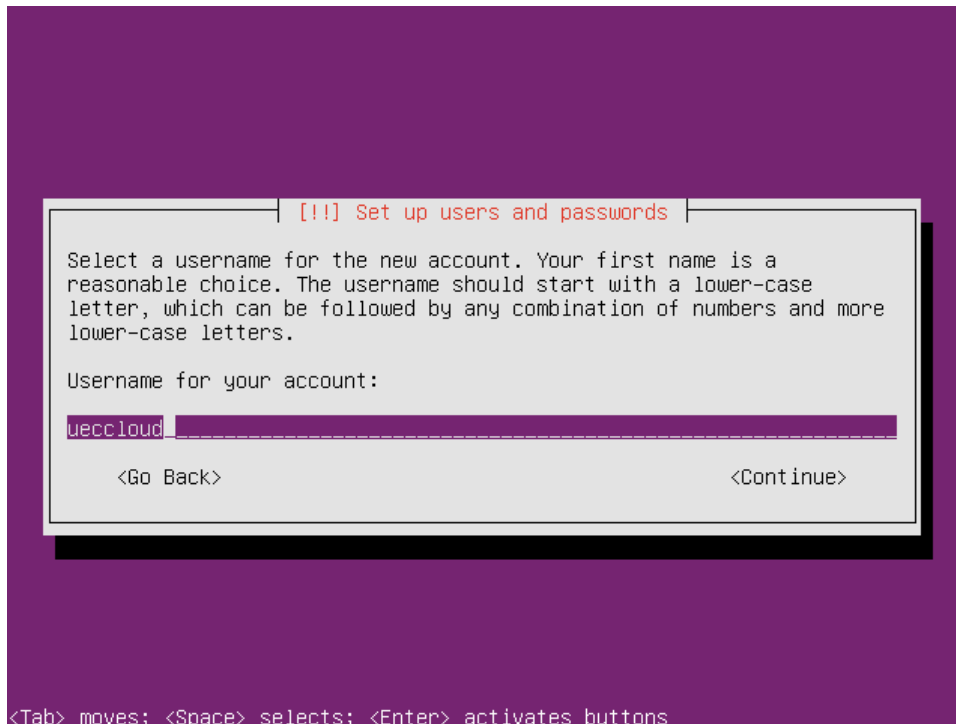


We should now set up the user. This user would be used to log on the server. Applying the principle of least privilege, we should not use administrative accounts (as root is) for non-administrative purposes. We would log on as this user, and when administrative work is needed to be done, we would elevate the privileges of this account using prefix "sudo", thus running commands as root.

First, choose the full name for the user – that is display name:

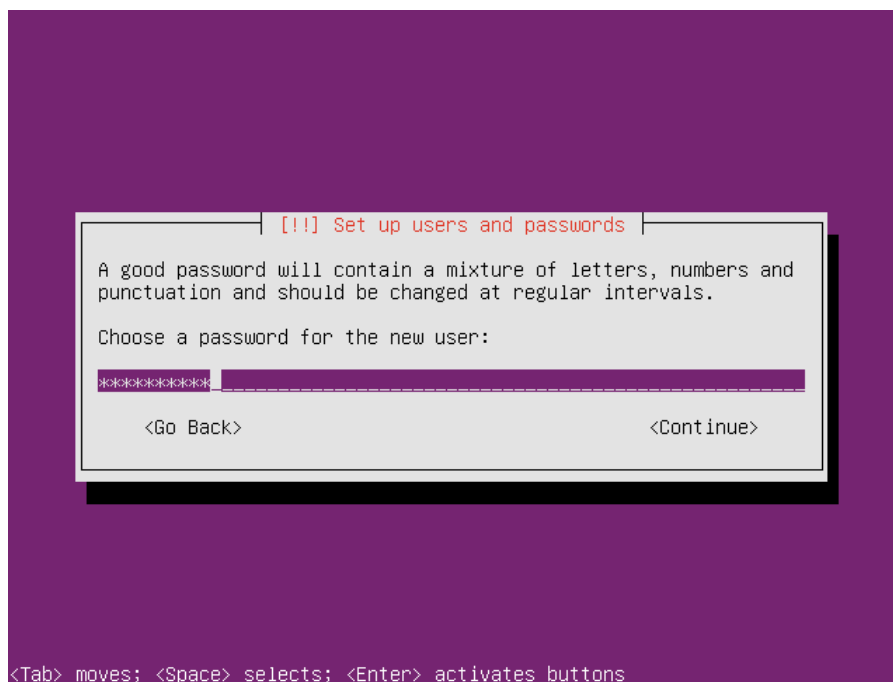


Choose the username for the account (bear in mind that usernames are case sensitive):



The screenshot shows a terminal window with a purple background. At the top, a title bar reads "[!!] Set up users and passwords". The main text in the terminal says: "Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters." Below this, it prompts "Username for your account:". A text input field contains the text "uecccloud". At the bottom of the terminal window, there are two buttons: "<Go Back>" on the left and "<Continue>" on the right. Below the terminal window, a legend states: "<Tab> moves; <Space> selects; <Enter> activates buttons".

Choose the password for the user:

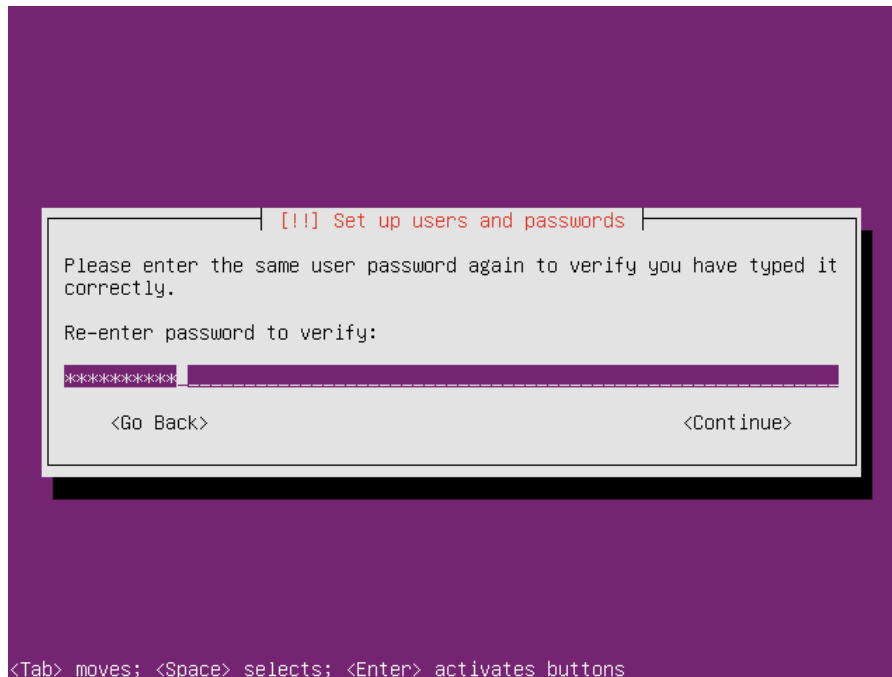


The screenshot shows a terminal window with a purple background. At the top, a title bar reads "[!!] Set up users and passwords". The main text in the terminal says: "A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals." Below this, it prompts "Choose a password for the new user:". A text input field contains a series of asterisks "*****". At the bottom of the terminal window, there are two buttons: "<Go Back>" on the left and "<Continue>" on the right. Below the terminal window, a legend states: "<Tab> moves; <Space> selects; <Enter> activates buttons".

In production environment it is recommended that the password is at least 16 characters long, and it should include at least one character from every of the four character groups (upper case letters, lower case letters, numbers, and special characters).

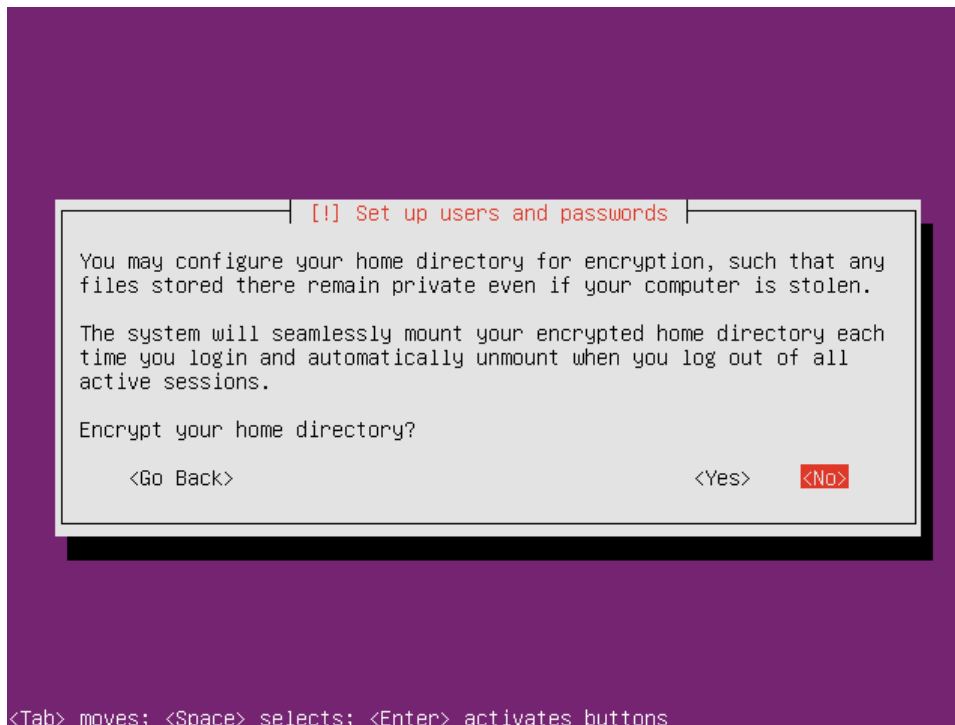
In our test environment (that is virtual and would never be upgraded to production system), we choose a simpler password for the sake of simplicity.

Repeat the password to make sure that it was typed correctly:



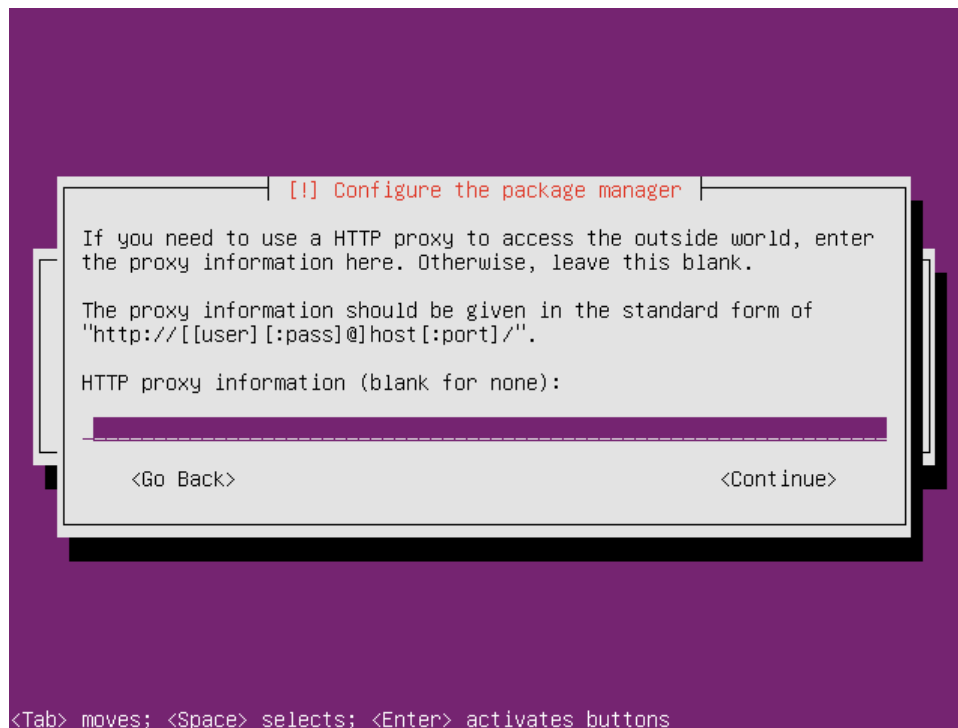
The screenshot shows a terminal window with a purple background. At the top, a title bar reads "[!] Set up users and passwords". The main text in the window says: "Please enter the same user password again to verify you have typed it correctly." followed by "Re-enter password to verify:". Below this is a password input field containing ten asterisks. At the bottom of the window are two buttons: "<Go Back>" on the left and "<Continue>" on the right. Below the terminal window, a legend states: "<Tab> moves; <Space> selects; <Enter> activates buttons".

We chose not to encrypt our home directory, since it is putting some overhead on processing power and storage. In production, if you expect that your home directory would host sensitive data, you would consider encrypting it.

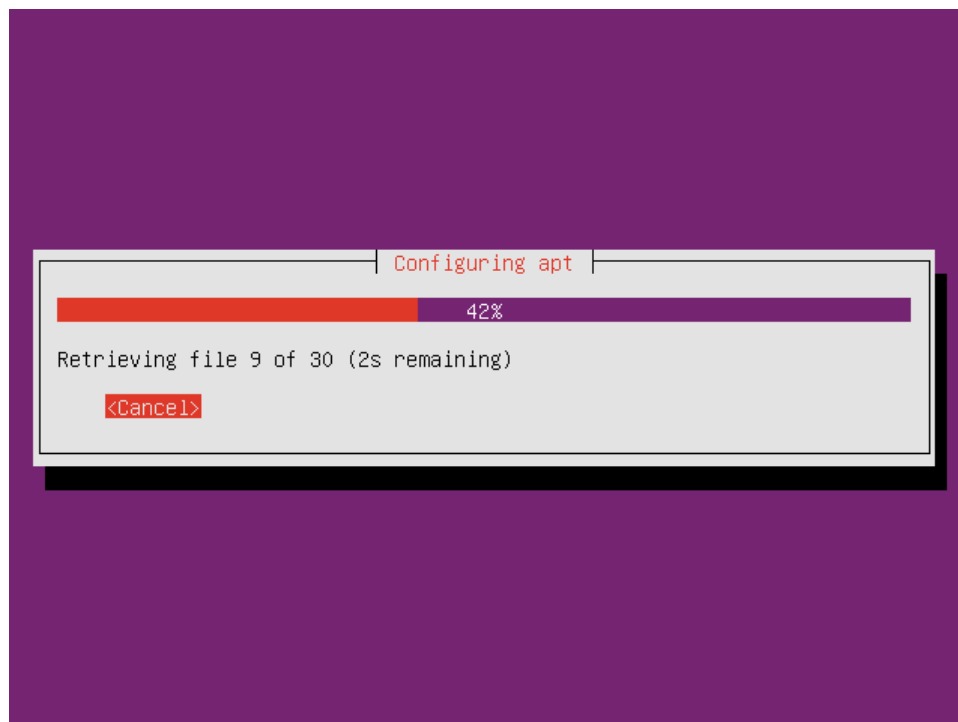


The screenshot shows a terminal window with a purple background. At the top, a title bar reads "[!] Set up users and passwords". The main text in the window says: "You may configure your home directory for encryption, such that any files stored there remain private even if your computer is stolen." followed by "The system will seamlessly mount your encrypted home directory each time you login and automatically unmount when you log out of all active sessions." Below this is the question "Encrypt your home directory?". At the bottom of the window are three buttons: "<Go Back>" on the left, "<Yes>" in the middle, and "<No>" on the right, which is highlighted with a red background. Below the terminal window, a legend states: "<Tab> moves; <Space> selects; <Enter> activates buttons".

If your internal network configuration includes proxy server for accessing the internet, add the proxy's address here:



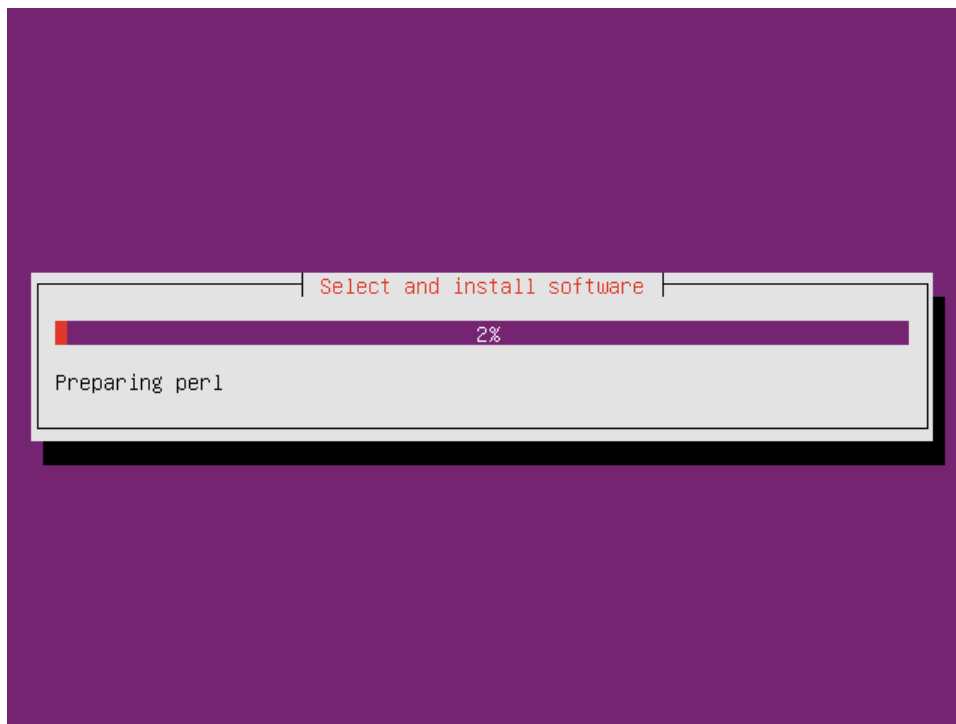
If no proxies used, leave the field blank, and choose to continue.
Configuring of Advanced Packaging Tool (APT)⁴ starts:



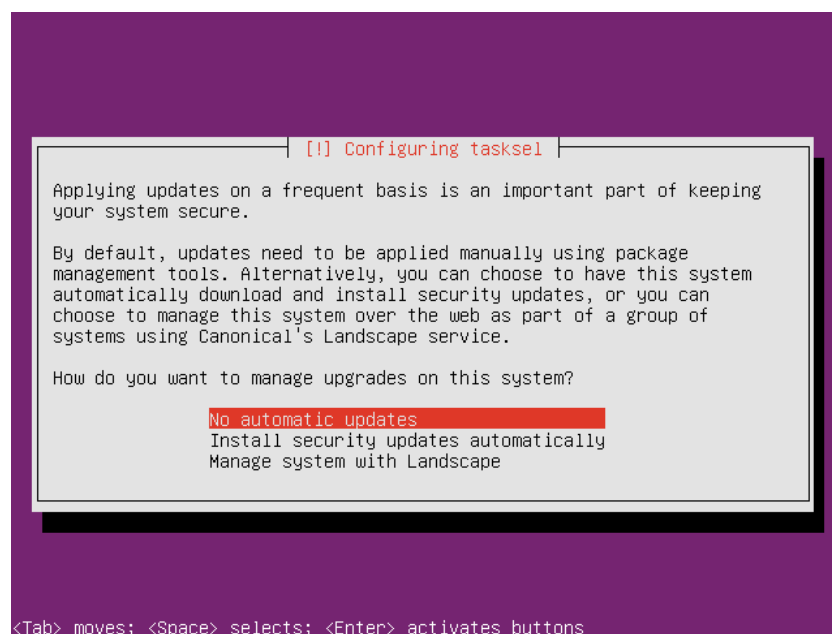
If the machine has access to the internet, packages are retrieved from there.

⁴ http://en.wikipedia.org/wiki/Advanced_Packaging_Tool

After configuring APT, preparation for the software installation starts:



Choose the setting for updating of your system. We would choose not to update the system automatically, since we would like to have a full control over the packages on the system. Otherwise the automatic update is an available option.

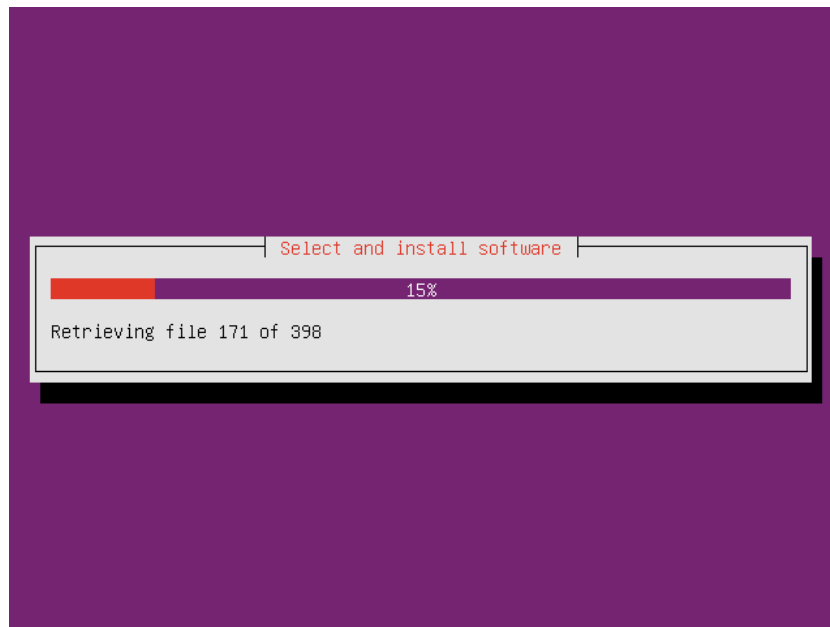


For production systems, choosing either no automatic updates, or managing the system with Landscape⁵ are valid options. Landscape is systems management and monitoring service provided by Canonical, and is a paid

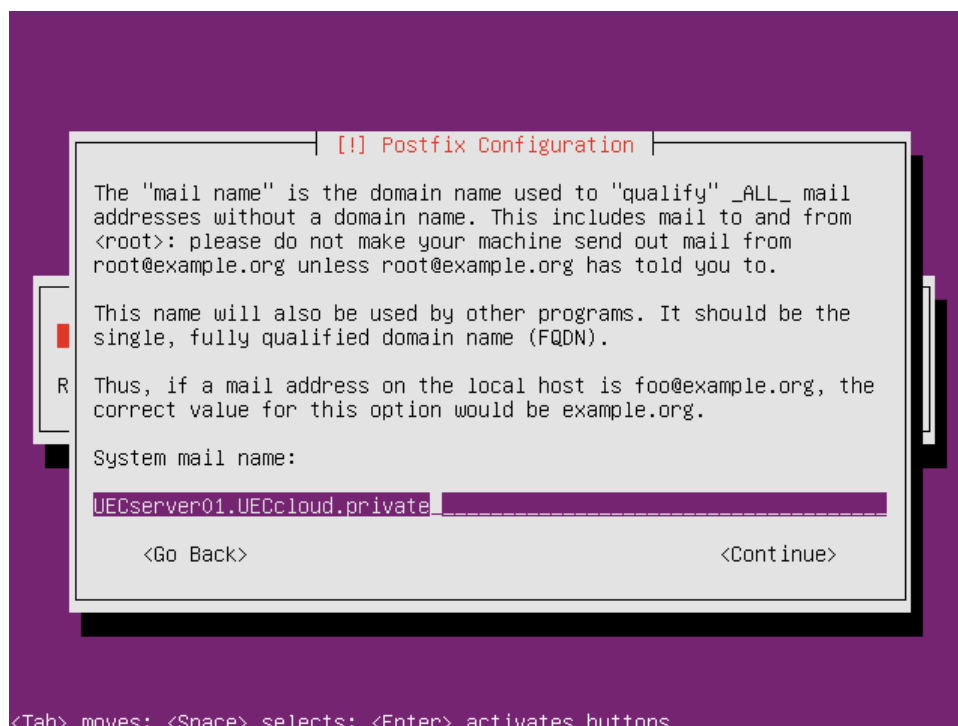
⁵ <https://landscape.canonical.com>

service for monitoring, managing and updating Ubuntu infrastructure using single interface, thus lowering management and administration costs.

Software installation starts. Again, this could take from just a few minutes to tens of minutes, since the files are being copied from the installations media to the hard drive, and how quick that would be done is depending on the speed of reading the installation media, and writing it on the disk.

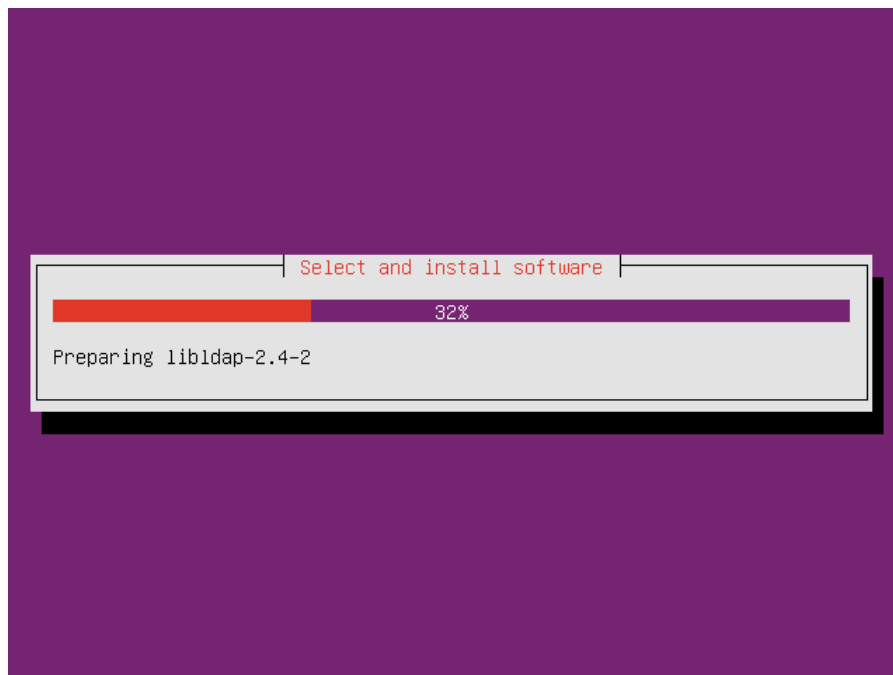


Mail (Postfix) configuration step is next, choosing the system mail name. Since we would not be using any public mail domain, we would configure a local "domain" i.e. "UECcloud.private":



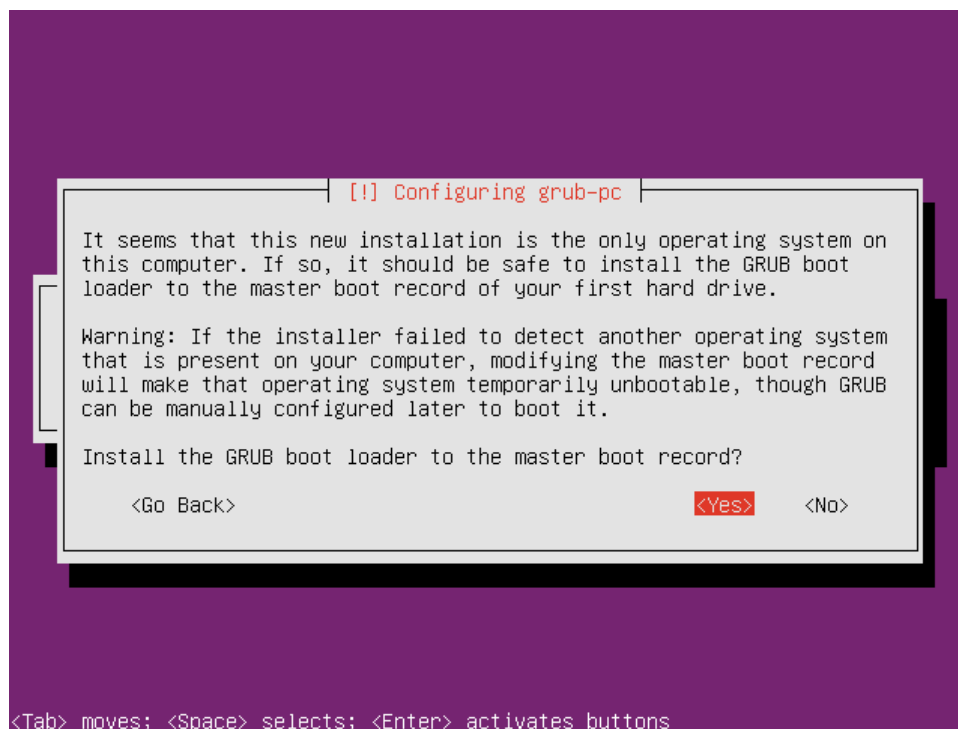
In production environment, you would choose to use your registered domain name (such as "itu.dk") to ensure the mail flow. Internal IT department would supply the required information.

Main installation starts:

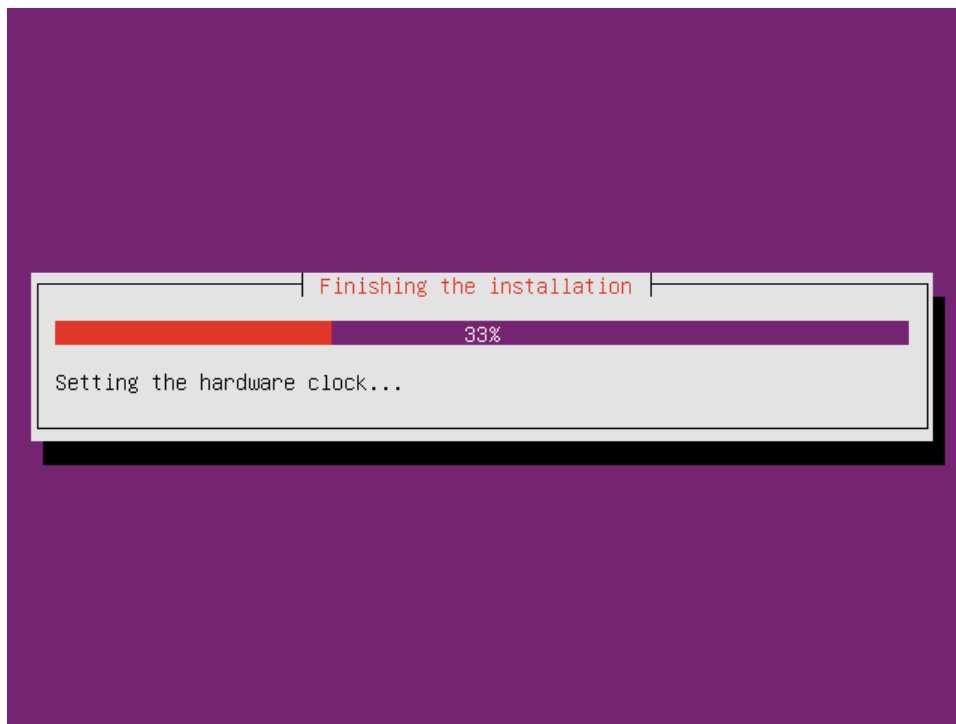


Again, this could take from just a few minutes to tens of minutes, since the files are being copied from the installations media to the hard drive, and how quick that would be done is depending on the speed of reading the installation media, and writing it on the disk.

Since the only operating system on our server would be Ubuntu server including UEC, we should choose to install boot loader, to make machine be able to boot from the disk:

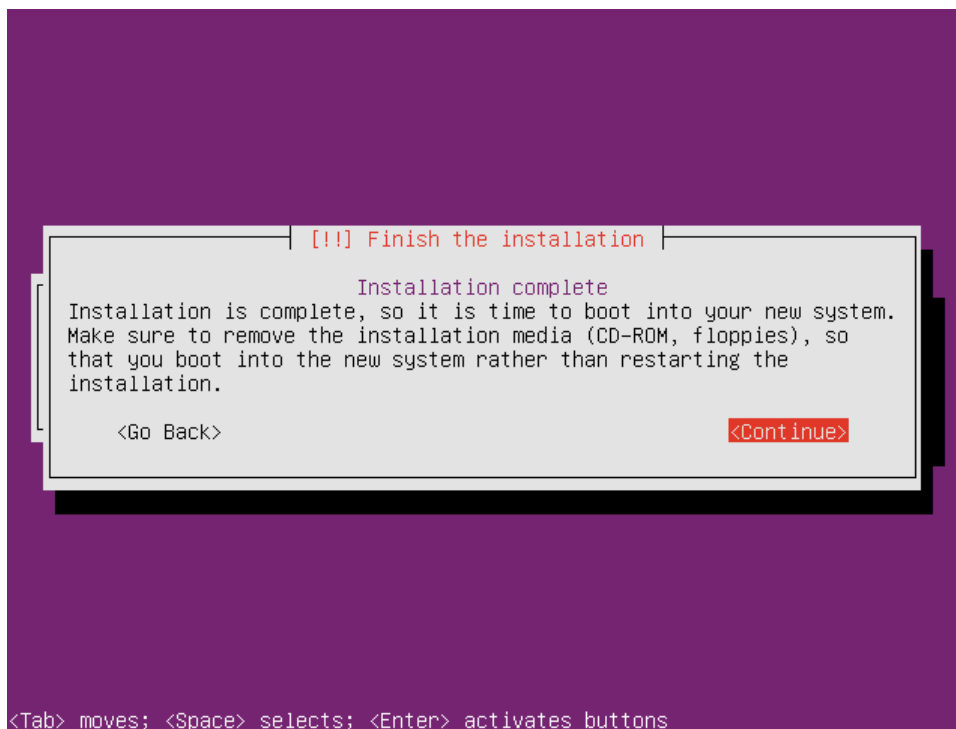


After that, the system is finishing the installation.



This includes several short steps, and should not take more than a few minutes.

Installation is completed:



Make sure that you un-mount / take out the installations media (CD), to prevent the system booting again into installation. If that happens, you just cancel the installation, take the media out, and recycle the machine – no damage to the installation is done.

After restart, the machine boots for the first time:

```
fsck from util-linux-ng 2.17.2
fsck from util-linux-ng 2.17.2
/dev/mapper/UECserver01-root: clean, 66171/12967936 files, 1129024/51841024 blocks
/dev/sda1: clean, 229/124496 files, 39133/248832 blocks
init: ureadahead-other main process (320) terminated with status 4
* Starting mDNS/DNS-SD daemon [ OK ]
* Stopping cold plug devices [ OK ]
* Stopping log initial device creation [ OK ]
* Starting load fallback graphics devices [ OK ]
* Starting save udev log and update rules [ OK ]
* Stopping load fallback graphics devices [ OK ]
* Starting Userspace boot splash [ OK ]
* Stopping save udev log and update rules [ OK ]
* Stopping Userspace boot splash [ OK ]
* Starting configure network device security [ OK ]
* Starting configure network device security [ OK ]
* Starting configure network device security [ OK ]
* Starting configure network device [ OK ]
* Starting Mount network filesystems [ OK ]
* Starting Eucalyptus network readiness [ OK ]
* Starting System V initialisation compatibility [ OK ]
* Stopping Mount network filesystems [ OK ]
* Stopping Eucalyptus network readiness [ OK ]
* Starting Bridge socket events into upstart [ OK ]
* Starting configure network device [ OK ]
* Starting configure network device security [ OK ]
* Starting configure virtual network devices [ OK ]
* Stopping configure virtual network devices [ OK ]
```

After the first login, you will meet this welcome screen, listing some information about the system running on your machine:

```
Ubuntu 11.04 UECserver01 tty1
UECserver01 login: uecccloud
Password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-server x86_64)

* Documentation:  http://www.ubuntu.com/server/doc

System information disabled due to load higher than 1.0

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

uecccloud@UECserver01:~$
```

System indicated that “*System information disabled due to load higher than 1.0*”. This is normal behavior after the first logon on the newly installed system. Booting up the first time, a considerable load is put on the system, and thus no processing power is left for composing and showing detailed system configuration.

Waiting for that initial system configuration after the first boot, or logging off and then on, the system information would be available:

```
Ubuntu 11.04 UECserver01 tty1
UECserver01 login: uecccloud
Password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-server x86_64)

* Documentation:  http://www.ubuntu.com/server/doc

System information as of Thu Jul 14 06:51:46 CEST 2011

System load:  0.35           Processes:           81
Usage of /:   0.6% of 194.65GB Users logged in:     0
Memory usage: 26%           IP address for eth0: 192.168.1.99
Swap usage:   0%

Graph this data and manage this system at https://landscape.canonical.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

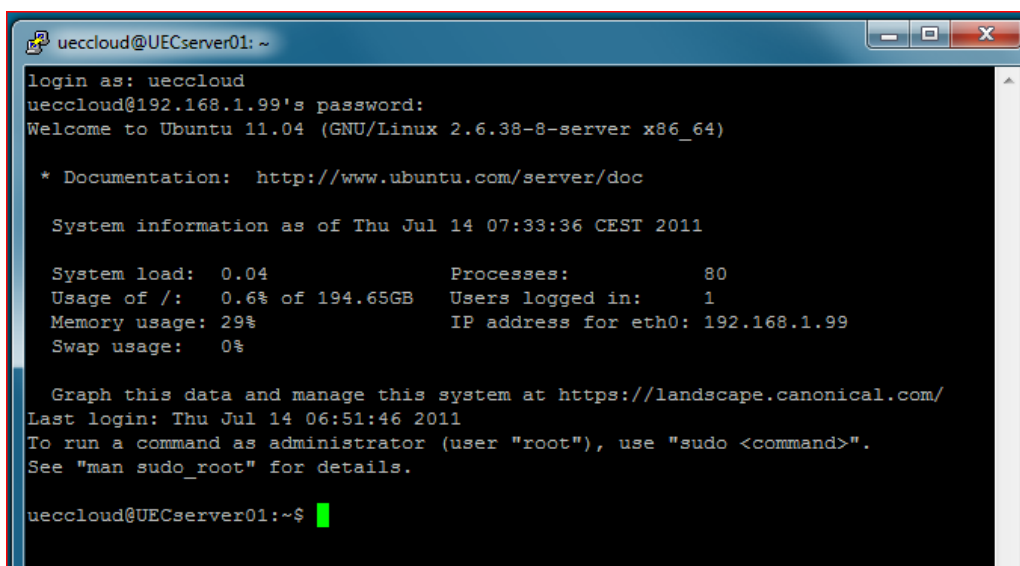
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

uecccloud@UECserver01:~$ _
```

From now on, a SSH session to the machine(s) is suggested, for several reasons. For the first, it is more convenient to work in just one interface (SSH terminal) than switching between several machine views. Next, you could use copy & paste option for the commands following the initial setup, during the post-installation steps. This way eventual misspelling would be avoided and configurations are performed faster.

I.e. from Windows, SSH application “PuTTY” can be used:



```
uecccloud@UECserver01: ~
login as: uecccloud
uecccloud@192.168.1.99's password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-server x86_64)

* Documentation:  http://www.ubuntu.com/server/doc

System information as of Thu Jul 14 07:33:36 CEST 2011

System load:  0.04           Processes:           80
Usage of /:   0.6% of 194.65GB Users logged in:     1
Memory usage: 29%           IP address for eth0: 192.168.1.99
Swap usage:   0%

Graph this data and manage this system at https://landscape.canonical.com/
Last login: Thu Jul 14 06:51:46 2011
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

uecccloud@UECserver01:~$
```

Be aware, though, that copying and pasting text with different coding (i.e. from Windows format to Linux) would eventually cause that some characters are not pasted, or pasted wrong. Please refer to the Appendix 4 about troubleshooting for more information.

Post installation steps

Set up static IP for both network interfaces. If the primary network interface was configured with DHCP during the installation, then set that interface to use static IP first. If you managed to set static IP during the installation, the configuration of only the secondary network interface is needed.

Public IP should be in 192.168.1.0 network, and private in 10.0.0.0 network.

Edit the network configuration of the server:

```
sudo vi /etc/network/interfaces
```

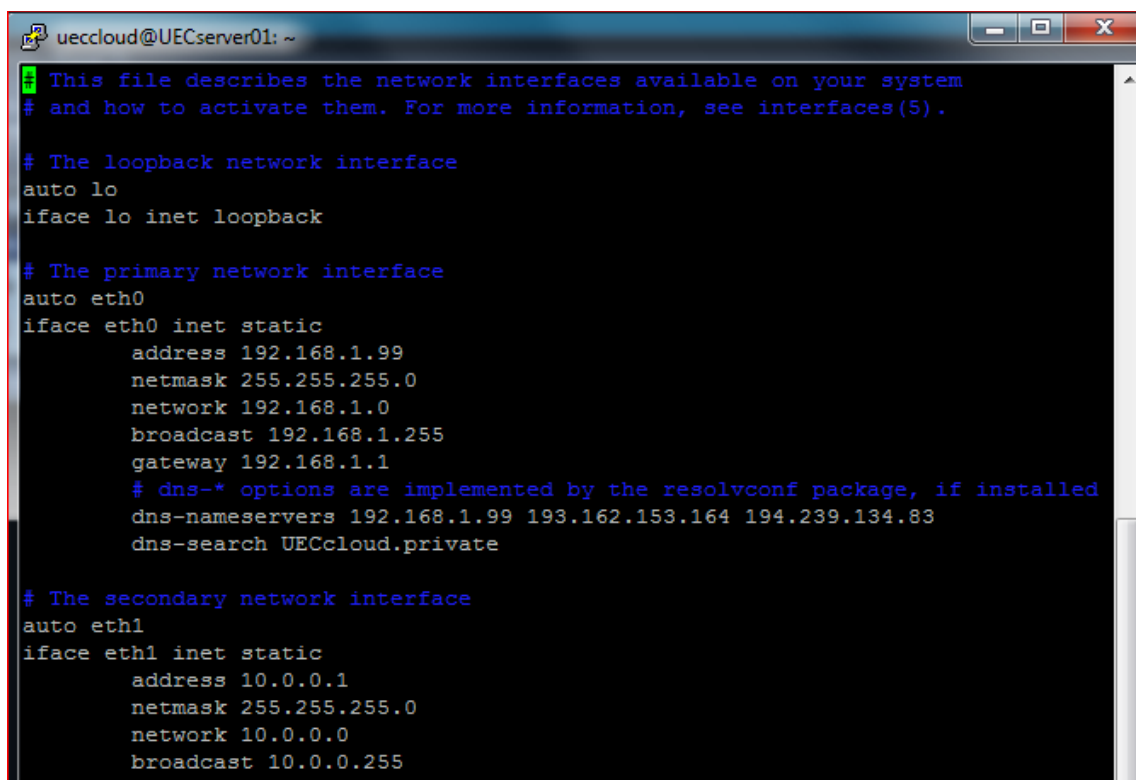
Under the primary network interface, remove the “dhcp” and configure it with static IP address:

```
auto eth0
iface eth0 inet static
    address 192.168.1.99
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
```

Add the secondary network interface that is to be configured with static IP address too:

```
auto eth1
iface eth1 inet static
    address 10.0.0.1
    netmask 255.255.255.0
    network 10.0.0.0
    broadcast 10.0.0.255
```

Your network configuration should now look like this:

A screenshot of a terminal window titled 'uecccloud@UECserver01: ~'. The terminal displays the contents of the /etc/network/interfaces file. The configuration includes a loopback interface 'lo' and two primary network interfaces, 'eth0' and 'eth1'. 'eth0' is configured with a static IP of 192.168.1.99, netmask 255.255.255.0, network 192.168.1.0, broadcast 192.168.1.255, and gateway 192.168.1.1. 'eth1' is configured with a static IP of 10.0.0.1, netmask 255.255.255.0, network 10.0.0.0, and broadcast 10.0.0.255. The terminal also shows comments about the resolvconf package and DNS settings.

```
uecccloud@UECserver01: ~
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.99
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
    # dns-* options are implemented by the resolvconf package, if installed
    dns-nameservers 192.168.1.99 193.162.153.164 194.239.134.83
    dns-search UECcloud.private

# The secondary network interface
auto eth1
iface eth1 inet static
    address 10.0.0.1
    netmask 255.255.255.0
    network 10.0.0.0
    broadcast 10.0.0.255
```

Restart the networking to apply the changes:
sudo /etc/init.d/networking restart

To be able to synchronize time between servers in the cloud, we will install NTP server on the first server, which will synchronize time with the external time source. All other servers in the cloud would synchronize the time with first server.

To set up NTP server, we have to install the NTP server first:
sudo apt-get install ntp
(if error "unable to locate package" occurs, run **sudo apt-get update**)

To make sure that the server will continue to serve the time even when off-line, a setting that makes it possible for the server to use its own clock as source should be made. This is done by opening the file **/etc/ntp.conf** and adding the following after the "# Specify one or more NTP servers" line:
server 127.127.1.0
fudge 127.127.1.0 stratum 10

Restart the NTP service afterwards to make the changes effective:
sudo /etc/init.d/ntp restart

Check server time:
date

Since first server has access to the internet through its public network, a router (Network Address Translation, NAT) will be installed⁶, to make it possible for the rest of the cloud servers that are only on the private network to connect to the outside network, for the purpose of i.e. fetching updates.

To set-up router, run the following commands:
sudo iptables -A FORWARD -o eth0 -i eth1 -s 10.0.0.0/24 -m conntrack --ctstate NEW -j ACCEPT
sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A POSTROUTING -t nat -j MASQUERADE
sudo iptables-save | sudo tee /etc/iptables.sav
sudo iptables-restore < /etc/iptables.sav
sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"

Edit the **/etc/sysctl.conf**:
uncomment **net.ipv4.ip_forward=1**
and add the following after the uncommented line:
net.ipv4.conf.default.forwarding=1
net.ipv4.conf.all.forwarding=1

Now run:
sudo iptables-save | sudo tee /etc/iptables.sav
Edit **/etc/rc.local** and add the following lines before the "exit 0" line:
iptables-restore < /etc/iptables.sav

To configure the gateway for routing between two interfaces (by enabling IP forwarding):
sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"

⁶ <http://ubuntuforums.org/showthread.php?t=713874>

Restart the server to apply the changes (can wait until all the initial settings are done):

sudo reboot

To make it easier to resolve the DNS names for the servers on the private network, and also for the first server itself, DNS server (BIND) should be installed. To do that, with default options, run the following command:

sudo apt-get install bind9

Check the DNS configuration `/etc/resolv.conf`:

The file should look like:

```
domain UECcloud.private  
search UECcloud.private  
# first contact the local DNS server installed on the same server  
nameserver 10.0.0.1  
nameserver 192.168.1.99  
# if that fails, contact the secondary servers (ISP's DNS)  
nameserver 193.162.153.164  
nameserver 194.239.134.83
```

To test that the local DNS is serving the DNS queries.

nslookup dr.dk

```
Server:          10.0.0.1  
Address:         10.0.0.1#53  
Non-authoritative answer:  
Name:   dr.dk  
Address: 195.137.194.128
```

If having troubles with DNS setup, please refer to Appendix 4 – troubleshooting.

To enable the servers to send mails, such as user verification mails, SMTP server should be installed. The default SMTP server for Ubuntu is Postfix⁷, and it is installed during the initial installation. To check or adapt the configuration, run the following command:

sudo dpkg-reconfigure postfix

Our setup is:

- Internet Site (mail sent directly using SMTP)
- UECserver01.UECcloud.private
- Enter admin mail address (in our case ueccloud@pantic.dk)
- Add eventual destinations, otherwise leave it like it is
- No
- Add local network 10.0.0.0/24 and 192.168.1.0/24
- Mailbox size limit – 0
- Leave “+”
- ipv4

The same could be done by editing `/etc/postfix/main.cf` (and others) as needed. After modifying main.cf, be sure to run '**sudo /etc/init.d/postfix reload**'.

Make sure that you have the latest version of Eucalyptus:

sudo apt-get update

⁷ <https://help.ubuntu.com/community/Postfix>

sudo apt-get upgrade eucalyptus

Depending on the version of your Eucalyptus and how many updates has been made since the release of your version, this process could take from several minutes to several tens of minutes, depending on the internet connection speed, and the speed of your hardware.

To check the version of Eucalyptus, view the following file:

/etc/eucalyptus/eucalyptus-version

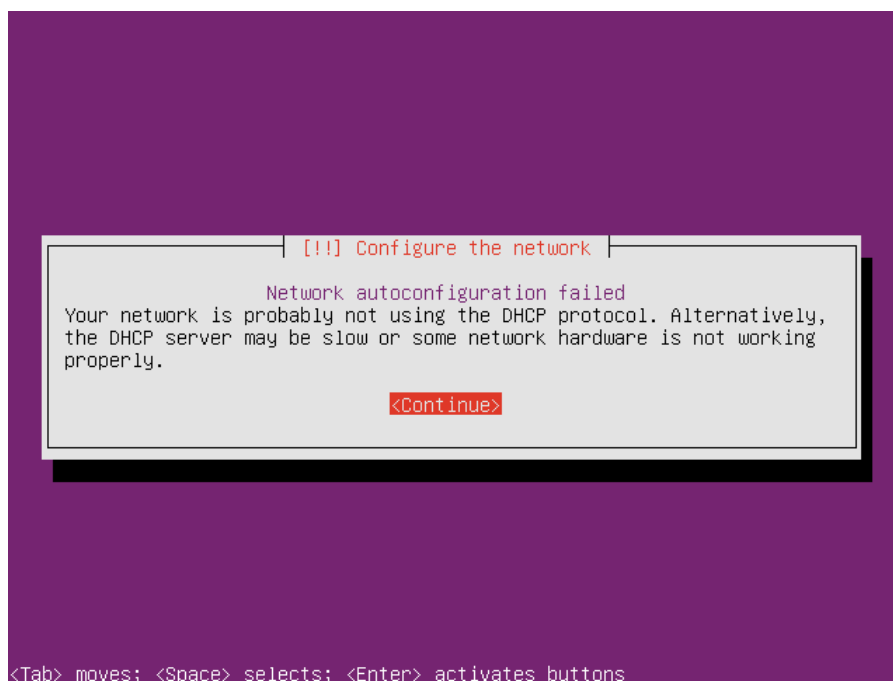
This is the last step of initial configuration for the first server in the cloud, and to make sure that the configuration is implemented, restart the machine (**sudo reboot**) and eventually check the installed features.

Installation of second server (CC, SC)

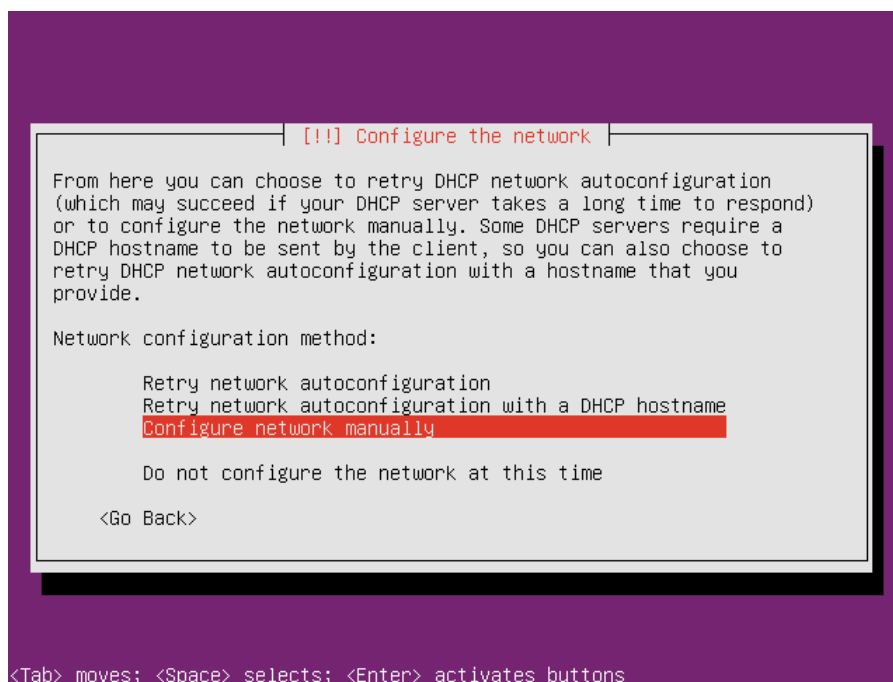
Mount the installation media, and boot from it. Choose the language – English. Follow the same steps as installing the first server, until you reach to the point of configuring the network.

If your network is configured with DHCP, stop the process (ESC) and jump to the step of configuring your network manually. (The servers should be configured with static IP addresses)

If your network is not configured with a DHCP server, then you will get a following error:



Choose to configure the network manually:



Set up static IP for the (public) network interface:

IP address 192.168.1.98

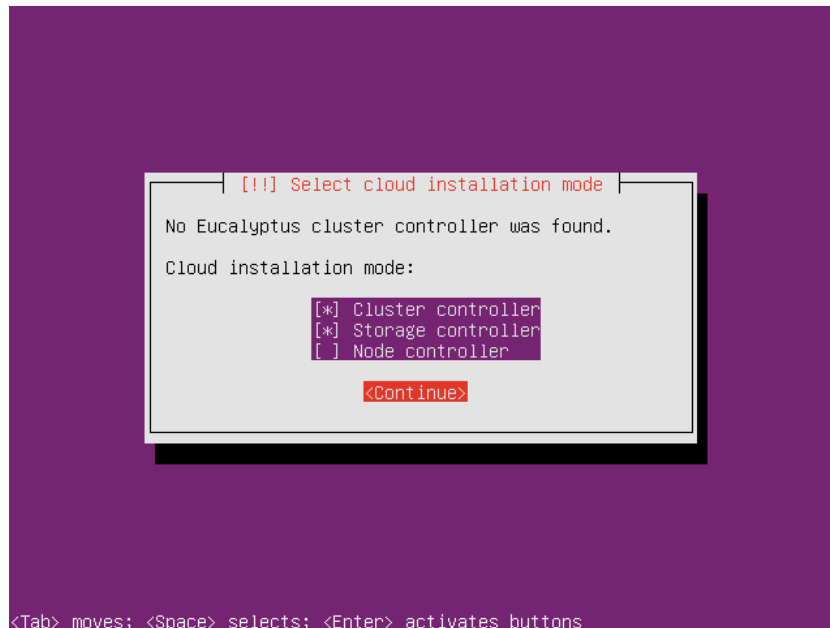
netmask 255.255.255.0

gateway 192.168.1.1

name server addresses: 192.168.1.99

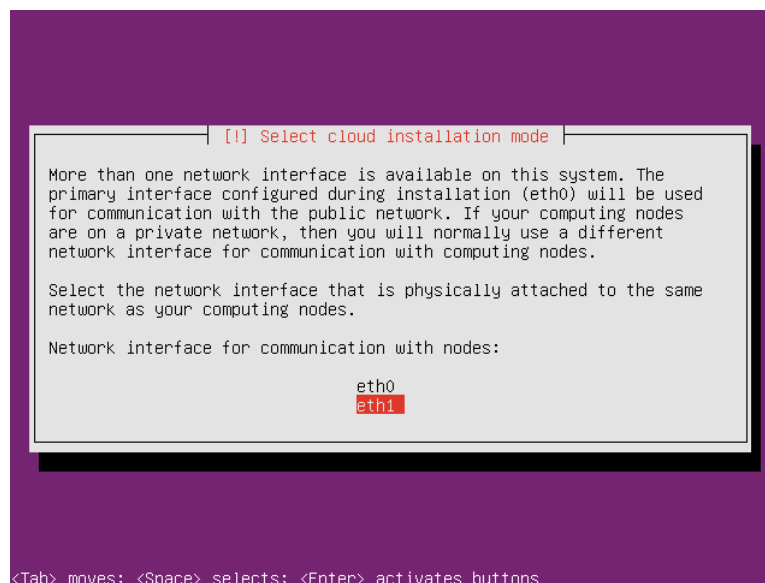
Write “UECserver02” for the hostname. For the domain name, write “UECcloud.private”.

The installation can contact the CLC and get information that the CLC and WS3 components are installed in the cloud, but there is no cluster configured yet. Choose to install the CC and SC components on the server:



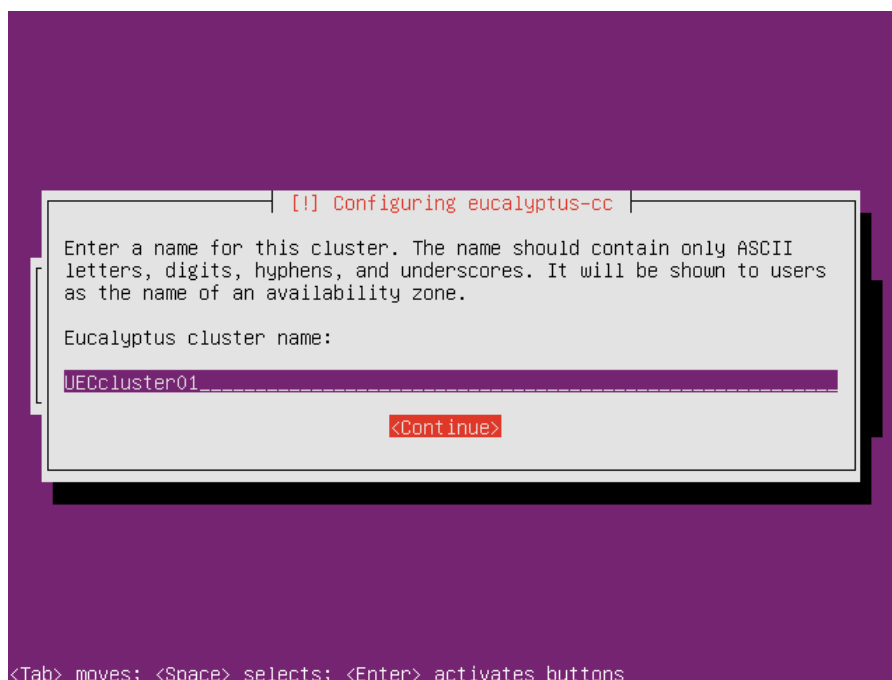
(If the installation complains that it cannot find a CLC or WS3, check the networking before going on!)

Since we have two network interfaces in the system, we should designate one that is to be used for communication with computing nodes (NCs). Since our computing nodes are going to be placed on the private network, we should choose the secondary network interface as the one used for communicating with nodes.



Configuring disks is done by following the same procedure as for the first server. Installing of the base system starts, after that the configuring of the APT, then installing the software.

Then, the installation reaches the point of configuring the cluster:



[!] Configuring eucalyptus-cc

Enter a name for this cluster. The name should contain only ASCII letters, digits, hyphens, and underscores. It will be shown to users as the name of an availability zone.

Eucalyptus cluster name:

UECcluster01

<Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Name the cluster as “UECcluster01”, since we are going to scale out the cloud later, adding another cluster.

Add the following pool of IP addresses: 192.168.1.100-192.168.1.199:



[!] Configuring eucalyptus-cc

Eucalyptus requires a pool of IP addresses that can be dynamically assigned as the "public" IPs of virtual machines. These IPs must be unused within their Class C subnet, this system must have an interface configured with an address on this subnet, and your prospective users must be able to connect to these IPs from wherever they run the client tools.

Please specify one or more ranges of IP addresses, e.g.:

192.168.1.100-192.168.1.199

or

192.168.2.50-192.168.2.99 192.168.2.150-192.168.2.199

You may leave this blank if you have no IP addresses available, BUT you and your users must then request the private addressing scheme when starting a virtual machine instance. For ec2-run-instances and euca-run-instances, this is done with the option "--addressing private".

192.168.1.100-192.168.1.199

<Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

(We are not taking the whole class C subnet, since we will use the rest of the addresses for the other cluster)

After the successful installation, the server reboots.

Post installation steps

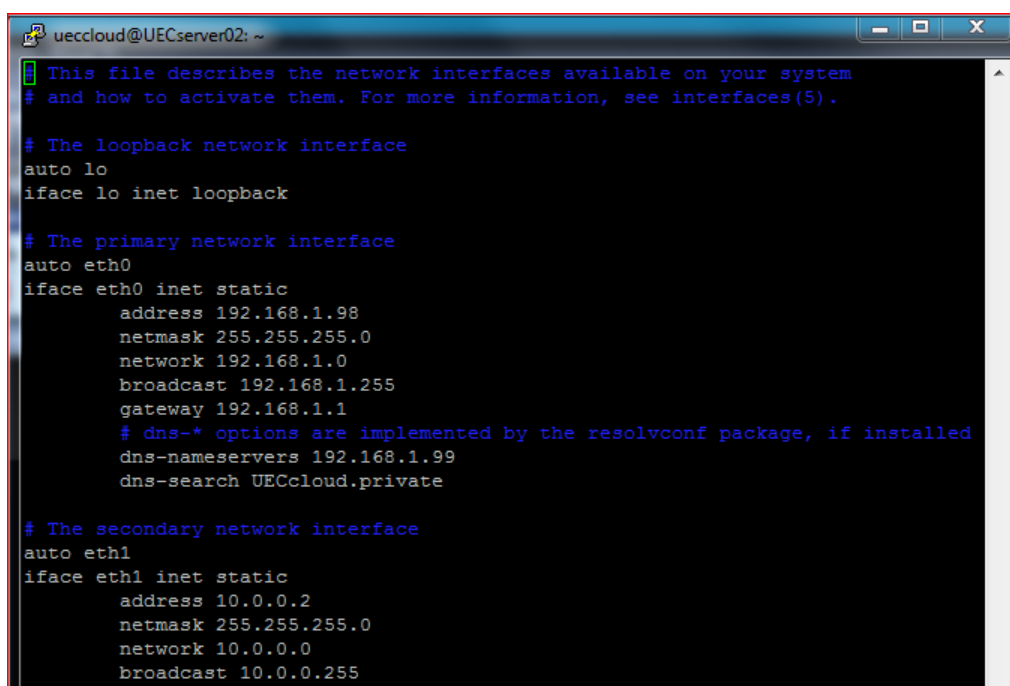
As a first step, check the configuration of the network interfaces, and set up static IP for the private network interface (eth1):

```
sudo vi /etc/network/interfaces
```

Add the following:

```
auto eth1  
iface eth1 inet static  
    address 10.0.0.2  
    netmask 255.255.255.0  
    network 10.0.0.0  
    broadcast 10.0.0.255
```

Your network configuration should now look like this:

A screenshot of a terminal window titled 'uecccloud@UECserver02: ~'. The terminal displays the contents of the /etc/network/interfaces file. The file contains configuration for three network interfaces: 'lo' (loopback), 'eth0' (primary), and 'eth1' (secondary). The 'eth1' interface is configured with a static IP of 10.0.0.2, netmask 255.255.255.0, network 10.0.0.0, and broadcast 10.0.0.255. The 'eth0' interface is configured with a static IP of 192.168.1.98, netmask 255.255.255.0, network 192.168.1.0, broadcast 192.168.1.255, gateway 192.168.1.1, and DNS settings. The 'lo' interface is configured as a loopback. The terminal text is as follows:

```
uecccloud@UECserver02: ~  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
auto eth0  
iface eth0 inet static  
    address 192.168.1.98  
    netmask 255.255.255.0  
    network 192.168.1.0  
    broadcast 192.168.1.255  
    gateway 192.168.1.1  
    # dns-* options are implemented by the resolvconf package, if installed  
    dns-nameservers 192.168.1.99  
    dns-search UECcloud.private  
  
# The secondary network interface  
auto eth1  
iface eth1 inet static  
    address 10.0.0.2  
    netmask 255.255.255.0  
    network 10.0.0.0  
    broadcast 10.0.0.255
```

Restart the networking to apply the changes:

```
sudo /etc/init.d/networking restart
```

To be able to synchronize the time on the server, we will install NTP:

```
sudo apt-get install ntp
```

(if error "unable to locate package" occurs, run **sudo apt-get update**)

To make the server synchronize the time with the first server, open the file **/etc/ntp.conf** and add:

```
server 10.0.0.1
```

Restart the NTP service afterwards to make the changes effective:

```
sudo /etc/init.d/ntp restart
```

Check server time:

```
date
```

Check the DNS configuration `/etc/resolv.conf` - it should look like:
`search UECcloud.private`
`nameserver 10.0.0.1`

Make sure that you have the latest version of Eucalyptus:

`sudo apt-get update`
`sudo apt-get upgrade eucalyptus`

To check the version of Eucalyptus, view the following file:

`/etc/eucalyptus/eucalyptus-version`

This is the last step of initial configuration for the second server in the cloud, and to make sure that the configuration is implemented, restart the machine (**`sudo reboot`**) and eventually check the installed features.

Installation of third server (NC)

Mount the installation media, and boot from it. Choose the language – English. Follow the same steps as installing the first server, until you reach to the point of configuring the network.

Choose to configure the network manually.

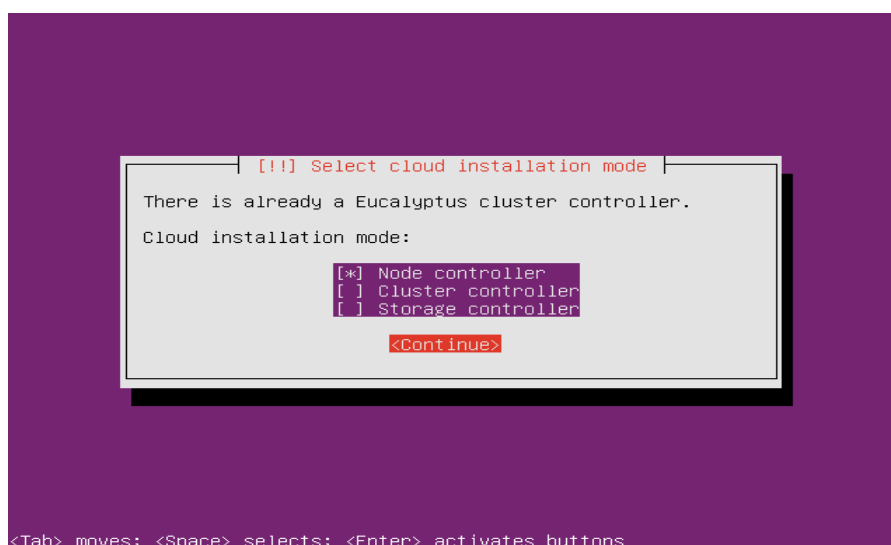
Set up static IP for the (private) network interface.

IP address 10.0.0.3
netmask 255.255.255.0
gateway 10.0.0.1
name server addresses: 10.0.0.1

Write “UECserver03” for the hostname.

For the domain name, write “UECcloud.private”.

The installation can contact the CLC and get information about CLC, WS3, CC and SC components are installed in the cloud, and offer to install the NC component on the server:



Configuring disks is done by following the same procedure as for the first server.

Installing of the base system starts, after that the configuring of the APT, then installing the software.

If you get the error about hardware not supporting virtualization acceleration, please check if your processor is VT-enabled (having VT extensions), and remember to turn that option on in BIOS.



(In our case, we get the error since we are installing UEC inside a virtual machine, where VT extensions are not supported)

After the successful installation, the server reboots.

Post installation steps

As a first step, check the configuration of the network interface (eth0):

sudo vi /etc/network/interfaces

Networking is implemented using bridging:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet manual

auto br0
iface br0 inet static
    address 10.0.0.3
    netmask 255.255.255.0
    network 10.0.0.0
    broadcast 10.0.0.255
    gateway 10.0.0.1
    # dns-* options are implemented by the resolvconf package, if installed
    dns-nameservers 10.0.0.1
    dns-search UECcloud.private
    bridge_ports eth0
    bridge_fd 9
    bridge_hello 2
    bridge_maxage 12
    bridge_stp off
```

To check network connectivity, try pinging an address that you positively know is giving response to ping requests.

To be able to synchronize the time on the server, we will install NTP:

sudo apt-get install ntp

(if error “unable to locate package” occurs, run **sudo apt-get update**)

To make the server synchronize the time with the first server, open the file **/etc/ntp.conf** and add:
server 10.0.0.1

Restart the NTP service afterwards to make the changes effective:
sudo /etc/init.d/ntp restart

Check server time:
date

Check the DNS configuration **/etc/resolv.conf** - it should look like:
search UECcloud.private
nameserver 10.0.0.1

Make sure that you have the latest version of Eucalyptus:
sudo apt-get update
sudo apt-get upgrade eucalyptus

To check the version of Eucalyptus, view the following file:
/etc/eucalyptus/eucalyptus-version

Restart the NC:
sudo restart eucalyptus-nc

This is the last step of initial configuration for the third server in the cloud, and to make sure that the configuration is implemented, restart the machine (**sudo reboot**) and eventually check the installed features.

Verifying the cloud installation

There is a row of verifying steps that could be performed to make sure that the cloud components were registered correctly. As of Ubuntu 10.04 LTS, all component registration should be automatic:

- Public SSH keys have been exchanged properly;
- The services are configured properly;
- The services are publishing their existence;
- The appropriate uec-component-listener is running;
- Verify Registration.

The steps mentioned above are needed if “Package Install” method is used. Since we are using “CD Install” method, we can skip those steps (or verify and perform a check if things are as they should be - please refer to the Appendix 4 about troubleshooting for more information on this).

Running the cloud

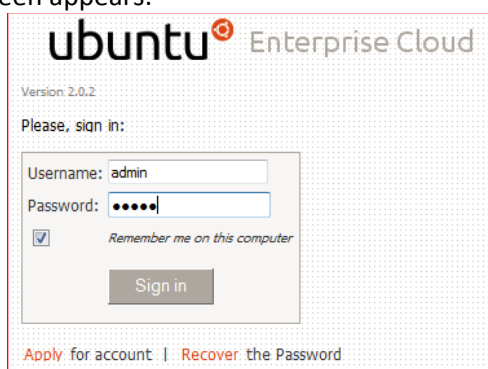
Now we have a cloud infrastructure installed on the server machines. Some initial administrative steps need to be performed to get the cloud up and running.

Cloud web interface

Finishing installing the three servers, our cloud is set up. Next step is connecting to the web interface of the UEC, and that is done by opening the following address in a browser: <https://192.168.1.99:8443>.

That address is a public address of our CLC, and the port “8443” is the default port.

After ignoring the certificate error (the issuer of the certificate is not in the trusted authorities on our client machine), the following logon screen appears:



The image shows the login screen for Ubuntu Enterprise Cloud. At the top, it says "ubuntu Enterprise Cloud" with the version "2.0.2" below it. The text "Please, sign in:" is followed by a form with fields for "Username: admin" and "Password: [masked]". There is a checkbox for "Remember me on this computer" and a "Sign in" button. At the bottom, there are links for "Apply for account" and "Recover the Password".

The default logon credentials are username “admin” and password “admin”. After logging on with those credentials, the next screen appears, where the password should be changed, administrator’s e-mail address should be given, and the CLC’s public IP address is guessed – make sure that the right public IP of the CLC is entered there.



The image shows the "First-time Configuration" screen for Ubuntu Enterprise Cloud. It asks the user to "Please, supply the following parameters to activate your Eucalyptus installation:". The form includes fields for "Administrator's new password:", "The password, again:", "Administrator's email address:" (with the value "admin@pantic.dk"), and "Cloud Host:" (with the value "192.168.1.99"). There is a "Submit" button at the bottom. A note at the bottom explains that the Cloud Host IP was guessed and should be correct, but it can be changed later.

After submitting, an admin web interface opens, with the possibilities for managing credentials, images, users, configuration, extras and store.

Configuration is opened first. Here is the info about cloud:

Cloud configuration:
Cloud Host:
Default kernel: Default ramdisk:

DNS configuration:
Domain name:
Nameserver: IP:

... about the WS3 configuration:

Walrus Configuration:

Walrus host:

Buckets Path:
Maximum bucket size (MB):
Maximum buckets per user:
Space reserved for unbundling images (MB):
Space reserved for snapshots (GB):

... about the cluster:

Clusters:

Name: UECcluster01

Cluster Controller
Host:
☒ Dynamic public IP address assignment
Reserve for assignment public IP addresses
Maximum of public IP addresses per user
Use VLAN tags through
Storage Controller

... and about VM types:

VM Types:

Name	CPUs	Memory (MB)	Disk (GB)
m1.small	<input type="text" value="1"/>	<input type="text" value="192"/>	<input type="text" value="2"/>
c1.medium	<input type="text" value="1"/>	<input type="text" value="256"/>	<input type="text" value="5"/>
m1.large	<input type="text" value="2"/>	<input type="text" value="512"/>	<input type="text" value="10"/>
m1.xlarge	<input type="text" value="2"/>	<input type="text" value="1024"/>	<input type="text" value="20"/>
c1.xlarge	<input type="text" value="4"/>	<input type="text" value="2048"/>	<input type="text" value="20"/>

Credentials

Managing credentials is where the user's Eucalyptus credentials can be downloaded as ZIP file. The public and private key pair that is downloaded as a part of the ZIP file can be used whenever X.509 certificates are required.

It is a good idea to download those credentials for the admin user, and save it on the client machine, and also make a backup of them. Click on "Download Credentials" button from the Credentials menu, and save the "euca2-admin-x509.zip" archive on your local machine. Unpack the archive.

Query interface credentials are two strings used with client tools for queries in which requests and parameters are encoded in URL. They can also be found in the file "eucarc" from the "euca2-admin-x509.zip" archive.

If users and admins would like to have a user interface for accessing both EC2 and their UEC private cloud, the cloud could be registered with the "Right Scale"⁸. Cloud URL should be the public IP address of the CLC, and there should be access to that IP address on the port "8443" from the internet (forwarding rule for the IP and the port combination should be made in the organization's firewall).

Images

Lists the images that are available locally on the cloud. Those images are downloaded from the "Store", or uploaded manually (custom images).

Users

Part of the web interface for administering users.

Configuration

This part presents the cloud configuration, with infrastructure information about the cloud.

Extras

List of Eucalyptus certified images, and compatible tools.

Store

Lists the standard images available from the image store.

⁸ <http://www.rightscale.com>

Initial steps

As a part of the initial setup via web interface, cloud admin should choose to perform the following steps:

- Change the password for the user “admin” (use strong password, and back it up at safe place)
- Check the cloud configuration found under “Configuration”, making sure that all the components are registered right
- Add users, both administrators and/or users
- Download and backup of credentials for user “admin” and other users
- Install image(s) available under “Store” – those images would appear under “Images” after downloading

Downloading user credentials

There are two ways for obtaining user credentials – via web, and from command line.

Make the `~/.euca` folder first:

```
mkdir -p ~/.euca
chmod 700 ~/.euca
cd ~/.euca
```

To obtain credentials from the web, click on the “Credential” tabs in web interface, and then on the button “Download credentials”.

Save the “euca2-admin-x509.zip” archive on your local machine, to `~/.euca` folder, and rename it to “mycreds.zip”. Unzip the file to the folder `~/.euca`:

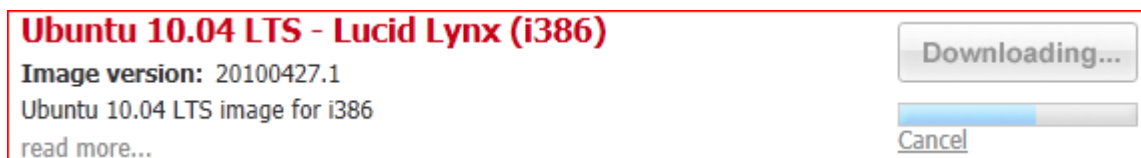
```
unzip -d ~/.euca mycreds.zip
cd -
```

The same can be done from command line on the CLC:

```
sudo euca_conf --get-credentials mycreds.zip
unzip mycreds.zip
ln -s ~/.euca/eucarc ~/.eucarc
cd -
```

Installing an image from the store

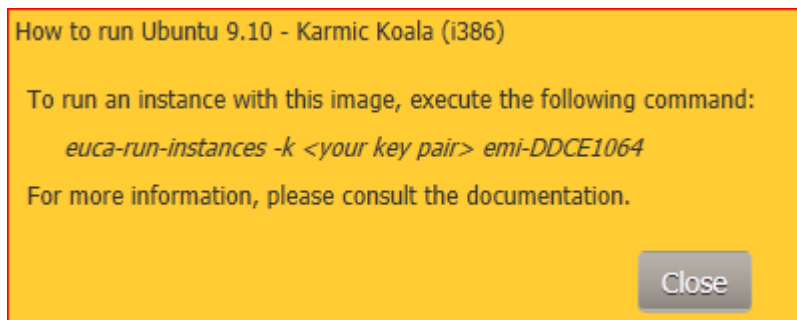
When clicking on the “Install” button, the image is downloaded locally to the cloud:



After an image is downloaded, its status is shown as “Installed”:



Information about running the image can be obtained by clicking on the “How to run?” link:



Running an image

There are several ways to instantiate an image in the UEC cloud:

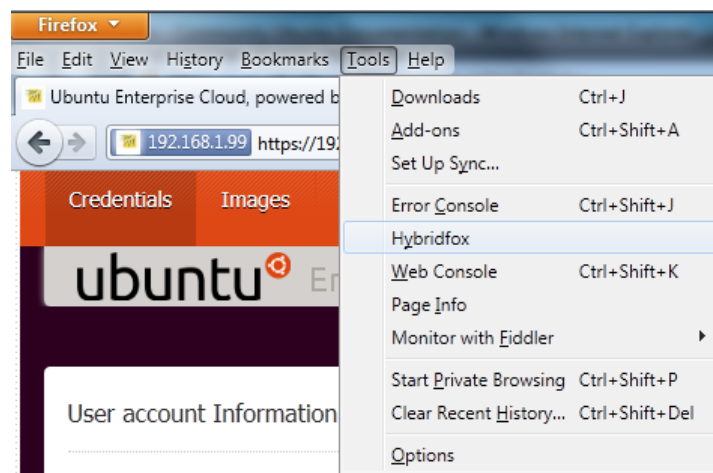
- Using HybridFox extension for Firefox,
- Using command line,
- Using Landscape, or another UEC compatible management tool (not covered in this document).

Using HybridFox

HybridFox (previously ElasticFox) is a web based GUI used to manage instances and other related aspects in the UEC. It is an extension for Mozilla’s Firefox, and can be downloaded⁹ and installed easily. HybridFox¹⁰ can connect to both public (Amazon) and private clouds (UEC).

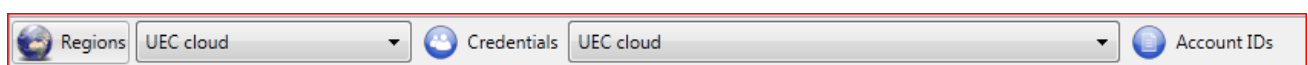
After installation, the browser should be restarted.

To start HybridFox, choose “HybridFox” from the “Tools” menu:



(In the newer versions of Firefox, press ALT to get the menu)

First you will need to define Regions, Credentials and Account IDs:



⁹ <http://code.google.com/p/hybridfox/downloads/list>

¹⁰ <https://help.ubuntu.com/community/HybridFox>

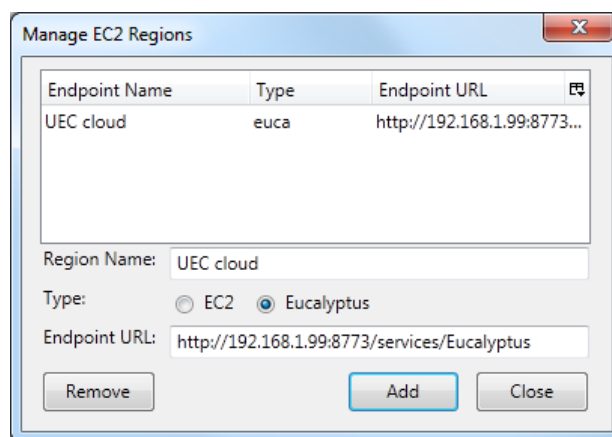
Information needed for setting these up can be found in the file “eucarc” from the downloaded credentials (euca2-admin-x509.zip that was renamed to mycreds.zip in our case), or in the web interface, under Credentials – “Query interface credentials”, clicking on the button “Show keys”.

In our example that info are:

```
Endpoint URL: http://192.168.1.99:8773/services/Eucalyptus
EC2_ACCESS_KEY='WKy3rMzOWPouVOxK1p3Ar1C2uRBwa2FBXnCw'
EC2_SECRET_KEY='J5ZGBb6bYv7z9ojPXHx0fGLLyIUcMck662K5Jg'
EC2_USER_ID='85280918035469249085443358232027004938'
```

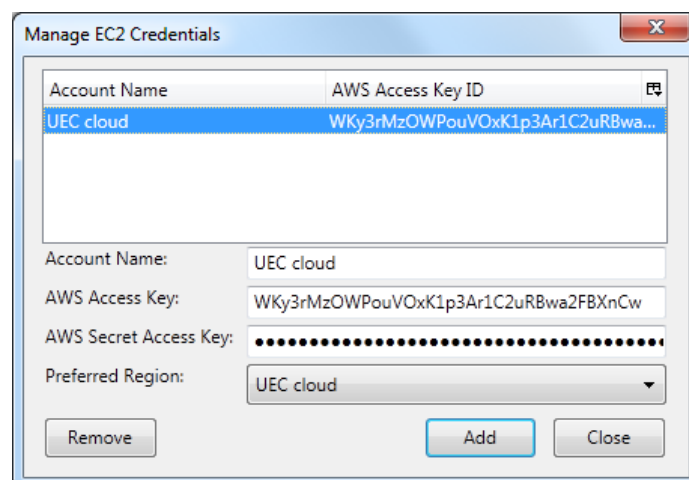
Define Regions:

Write the region name at your choice, best describing your cloud. Type should be Eucalyptus, and endpoint URL is <http://<cloud-IP-address>:8773/services/Eucalyptus> - click on Add, and then on Close:



Define Credentials:

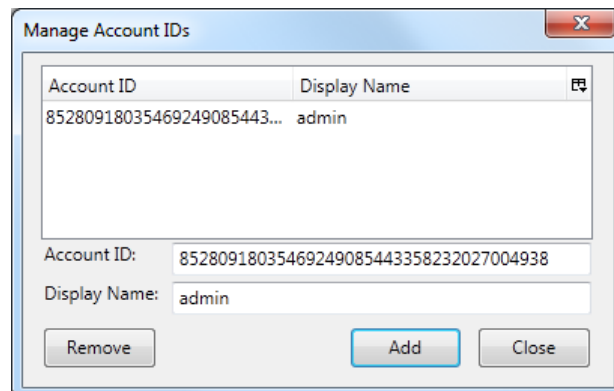
Fill in the account name at your choice, best describing your account name. AWS access key is EC2_ACCESS_KEY, and AWS Secret Access Key is EC2_SECRET_KEY. Choose your region from the drop-down menu (the one you just defined in the previous step):



Click on Add, and then on Close.

Define Account IDs:

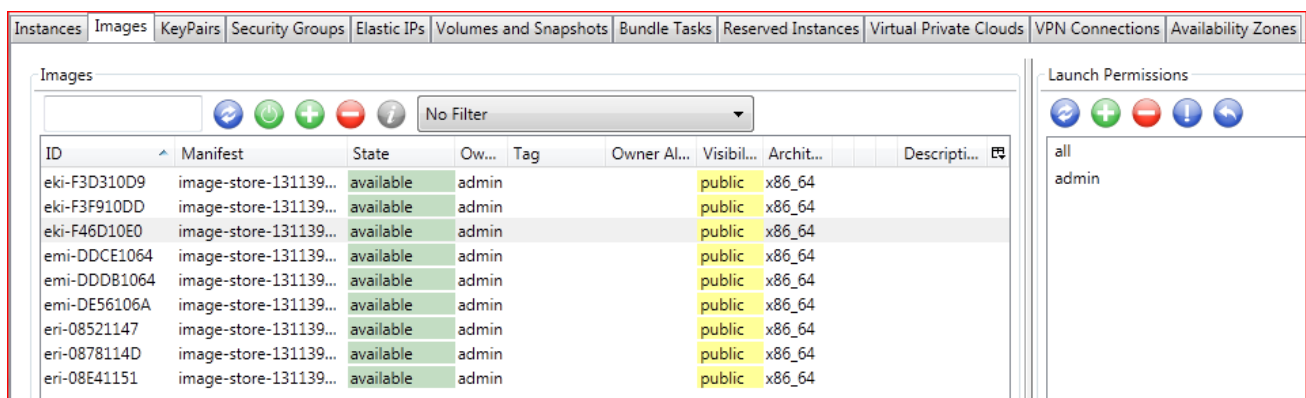
Fill in the account ID, which is EC2_USER_ID. Choose the display name best describing your account:



Click on Add, and then on Close.

After setting that up, you would probably need to close and reopen the HybridFox tab in Firefox.

When HybridFox is started again, in the initial view you should be able to see the images you downloaded from the store:



Here is a short description of the options available (the tabs) that could be used for UEC cloud:

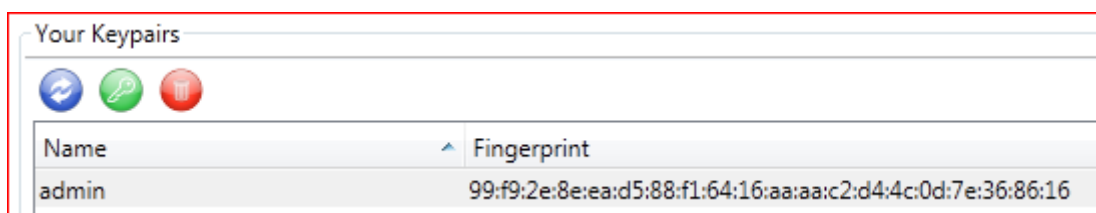
- Instances:
 - List over instances and their statuses; there are several administrative options (like terminating, showing console output ...),
- Images:
 - Listing over available images, with several administrative options (launch, register AMI ...),
- Key Pairs:
 - Lists the key pairs, with few administrative options,
- Security Groups:
 - Lists the security groups, with few administrative options,
- Elastic IPs:
 - Lists public IP addresses available to instantiated instances, with several administrative options (allocate, release, associate ...),
- Volumes and Snapshots:
 - Gives possibility to create volumes with options (create, delete, attach, detach ...) and manage snapshots (create new volume from, delete ...),

- Bundle tasks:
Lists bundled tasks, with few administrative options,
- Availability zones:
Lists the clusters available.

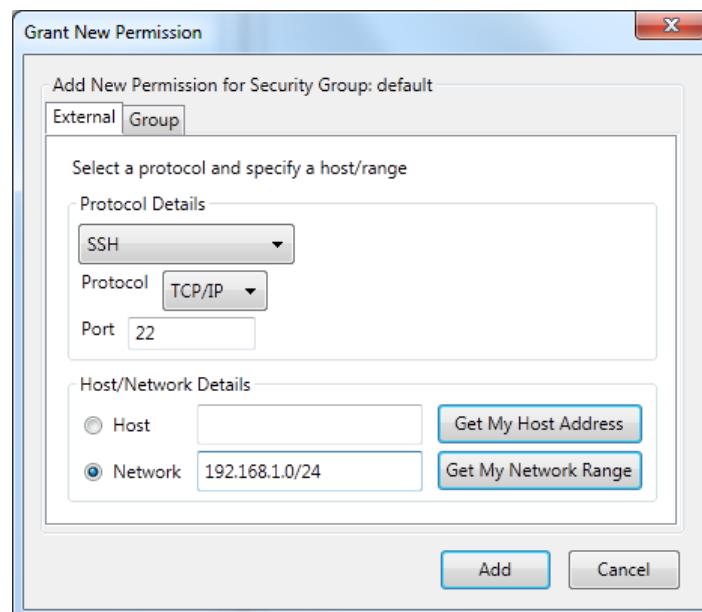
Reserved Instances, Virtual Private Clouds and VPN Connections tabs are not functional in UEC as the services are not implemented.

Additional steps to be done before we can start using the cloud from the HybridFox:

- Create key pair:
On Linux machines with Firefox installed, this key pair is usually already there, so the only thing is refreshing the view; on Windows machines (or generally, if it was not already installed), one should click on “Create a new key pair”, and provide the name for the key pair; afterwards, the .pem (certificate) file should be saved locally on the machine; when done, it should look somewhat like:

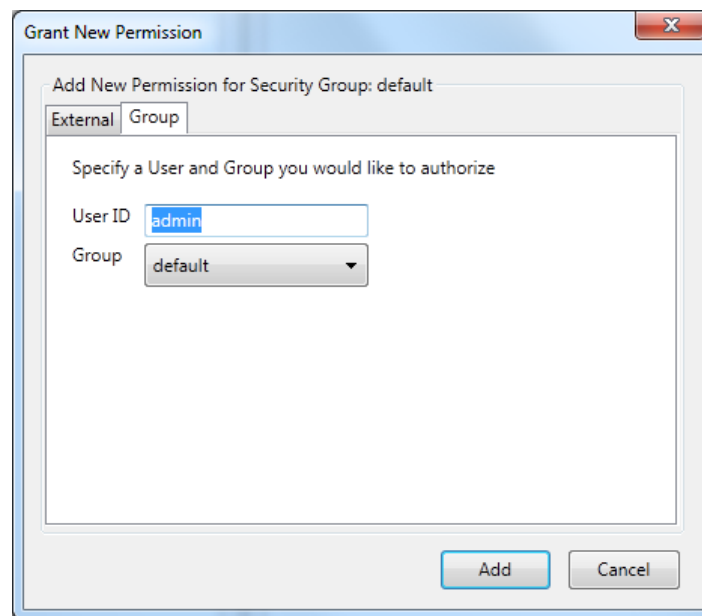


- Grant permission to the default security group:
Select the security group, and then click on the button “grant permission”:








Choose the protocol to be allowed, and from which host / network.

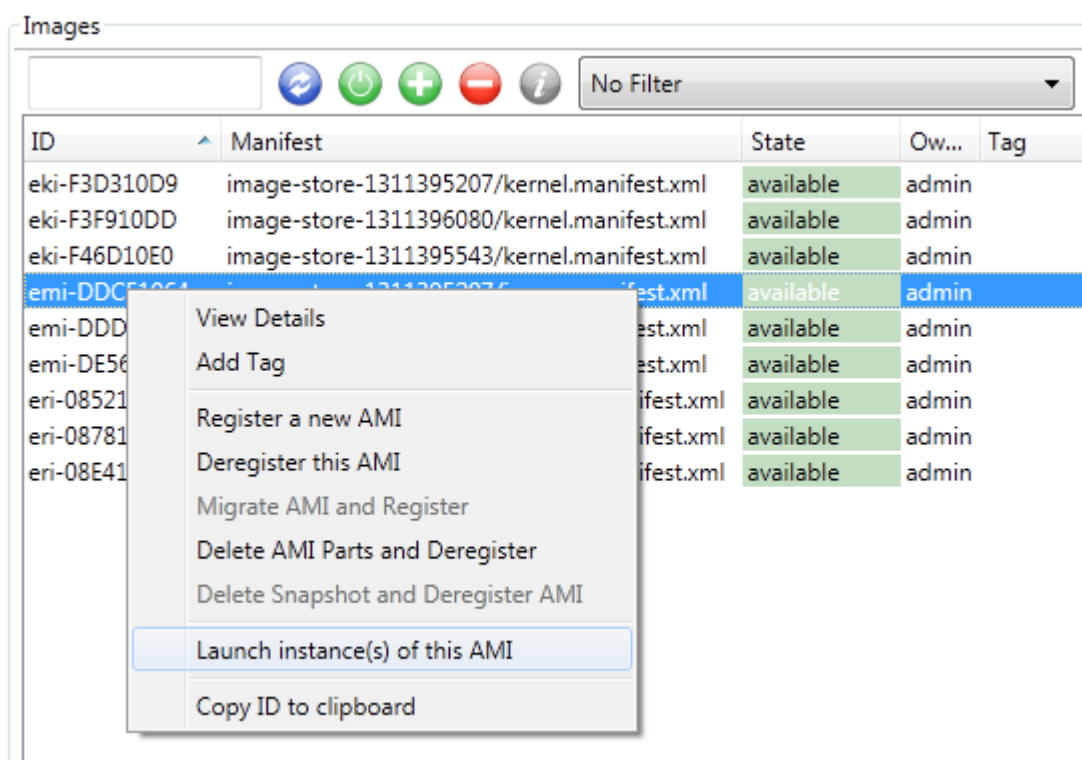
On the group tab, specify the user and the group to be authorized:



After adding, permissions should look something like this:

Your Groups			Group Permissions				
  			 				
Owner	Name	Description	Protocol	From Port/ICMP Type	To Port/ICMP Code	Source User/Group	Source CIDR
admin	default	default group	tcp	22	22		192.168.1.0/24

Now we are ready to instantiate an instance. Right click on an image of type “image.manifest.xml”, and click on “Launch instance(s) of this AMI”:



In the dialog box coming, you can leave it as it is default, to run the machine with the “small” instance type. Otherwise, choose another instance type. Availability zone defines on what cluster the instance would be instantiated. When finished setting up, click on “Launch”.

The 'Launch new instance(s)' dialog box includes the following fields and options:

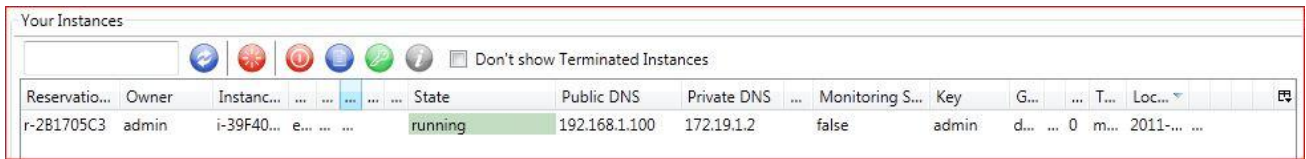
- AMI ID: emi-DDCE1064
- AMI Tag: (empty)
- AMI Manifest: image.manifest.xml
- AKI ID: eki-F3D310D9
- ARI ID: eri-08521147
- Instance Type: m1.small
- Number of instances - Min: 1, Max: 1
- New Instance(s) Tag: (empty)
- KeyPair: admin
- Availability Zone: <any>
- Additional Info: (empty)
- Public Address: ☒
- Override Root Volume Size: (empty)
- Virtual Private Cloud:
 - Launch in VPC: ☐
 - VPC: (empty)
 - Subnet: (empty)
 - IP Address: (empty)
- Security Groups:
 - Available Groups: (empty)
 - Launch in: default
- User Data: (empty text area)
 - Open File
 - Open Binary File
- Buttons: Launch, Cancel

Switch to the “Instances” tab. Your instance should be listed there, with status “pending”:

Your Instances													
<div> <input type="checkbox"/> Don't show Terminated Instances </div>													
Reservatio...	Owner	Instanc...	State	Public DNS	Private DNS	...	Monitoring S...	Key	G...	T...
r-2B1705C3	admin	i-39F40...	e...	pending	192.168.1.100	172.19.1.2		false	admin	d...	0 m...

Now the image is transferred over network to the NC that is going to run the instance, and this can take some time (minutes on 100 Mbit/s network, shorter on gigabit networks).

After that, your instance's state would change to "running":



The screenshot shows the 'Your Instances' page in the AWS Management Console. It features a table with columns: Reservation ID, Owner, Instance ID, State, Public DNS, Private DNS, Monitoring Status, Key Pair, Group, Tenancy, and Location. A single instance is listed with ID 'i-39F40...', state 'running', public DNS '192.168.1.100', and private DNS '172.19.1.2'. The 'Monitoring S...' column shows 'false'.

Reservation...	Owner	Instanc...	State	Public DNS	Private DNS	...	Monitoring S...	Key	G...	...	T...	Loc...
r-2B1705C3	admin	i-39F40...	e...	...	running	192.168.1.100	172.19.1.2		false	admin	d...	...	0	m... 2011-...

If you get an error, or your instance doesn't start, but goes directly to "terminated" after "pending", please refer to the Appendix 4 about troubleshooting.

Right click on the running instance, and choose "Connect to instance" – that will make a SSH session to your instance.

Using command line

First, make sure that you created key pairs. If you didn't do it by now, run the following:

```
mkdir -p -m 700 ~/.euca
touch ~/.euca/mykey.priv
chmod 0600 ~/.euca/mykey.priv
euca-add-keypair mykey > ~/.euca/mykey.priv
```

Verify you keypair:

```
euca-describe-keypairs
```

That should list your "mykey" keypair that you just created.

Allow access via SSH (port 22) to the instances:

```
euca-authorize default -P tcp -p 22 -s 0.0.0.0/0
```

Instantiate an instance of your registered image using "euca-run-instances \$EMI -k your_keypair -t instance_size", in our case it would be something like:

```
euca-run-instances emi-DDCE1064 -k mykey -t m1.xlarge
```

To monitor the state of the instance, run:

```
watch -n5 euca-describe-instances
```

To determine which IP address the instance got:

```
IPADDR=$(euca-describe-instances | grep $EMI | grep running | tail -n1 | awk '{print $4}')
```

Connect to your instance:

```
ssh -i ~/.euca/mykey.priv admin@$IPADDR
```

Scaling out the cloud – adding NC to a cluster

If we needed some more computing power in our cluster, i.e. if we were often getting messages about not having resources enough when we wanted to instantiate an instance, we would need to add one or more NC's to the cluster.

Installation of fourth server (NC)

In our set-up, we would add one NC to the existing cluster “UECcluster01”.

The NC would be based on this hardware:

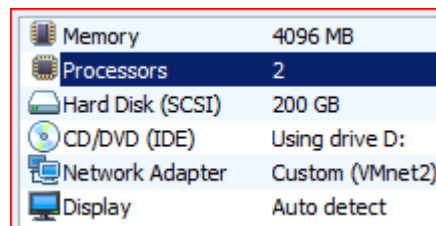
UECserver04

Roles: NC

Processor architecture: 64 bit

VT: VT enabled

Network: private (VMnet2)

A screenshot of a virtual machine hardware configuration window. It lists various components and their settings. The 'Processors' row is highlighted in blue. The window has a red border.

Memory	4096 MB
Processors	2
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using drive D:
Network Adapter	Custom (VMnet2)
Display	Auto detect

Mount the installation media, and boot from it. Choose the language – English.

Follow the same steps as installing other servers, until you reach to the point of configuring the network.

Choose to configure the network manually.

Set up static IP for the (private) network interface.

IP address 10.0.0.4

netmask 255.255.255.0

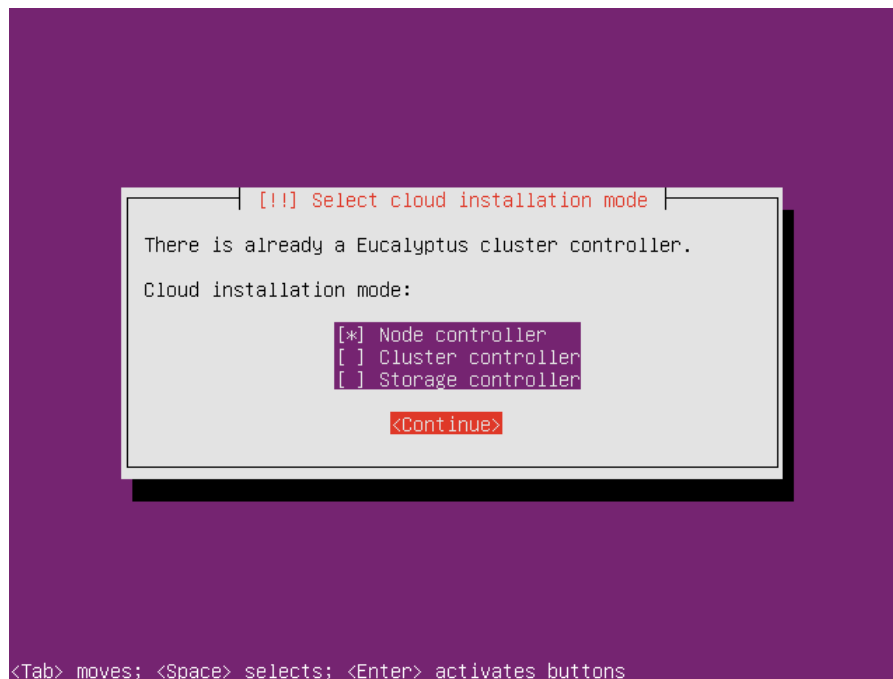
gateway 10.0.0.1

name server addresses: 10.0.0.1

Write “UECserver04” for the hostname.

For the domain name, write “UECcloud.private”.

The installation can contact the CLC and get information about CLC, WS3, CC and SC components are installed in the cloud, and offer to install the NC component on the server:



Configuring disks is done by following the same procedure as for the first server.

Installing of the base system starts, after that the configuring of the APT, then installing the software.

Again, if you get the error about hardware not supporting virtualization acceleration, please check if your processor is VT-enabled (having VT extensions), and remember to turn that option on in BIOS.
(In our case, we get the error since we are installing UEC inside a virtual machine, where VT extensions are not supported)

After the successful installation, the server reboots.

Post installation steps

As a first step, check the configuration of the network interface (eth0):

sudo vi /etc/network/interfaces

(Networking is implemented using bridging.)

To check network connectivity, try pinging an address that you positively know is giving response to ping requests.

To be able to synchronize the time on the server, install NTP:

sudo apt-get install ntp

(if error "unable to locate package" occurs, run **sudo apt-get update**)

To make the server synchronize the time with the first server, open the file **/etc/ntp.conf** and add:

server 10.0.0.1

Restart the NTP service afterwards to make the changes effective:

```
sudo /etc/init.d/ntp restart
```

Check server time:

```
date
```

Check the DNS configuration `/etc/resolv.conf` - it should look like:

```
search UECcloud.private  
nameserver 10.0.0.1
```

Make sure that you have the latest version of Eucalyptus:

```
sudo apt-get update  
sudo apt-get upgrade eucalyptus
```

To check the version of Eucalyptus, view the following file:

```
/etc/eucalyptus/eucalyptus-version
```

Restart the NC:

```
sudo restart eucalyptus-nc
```

This is the last step of initial configuration for the third server in the cloud, and to make sure that the configuration is implemented, restart the machine (**sudo reboot**) and eventually check the installed features.

Now that we added a node to our existing cluster, we can see it:

```
sudo euca_conf --list-nodes
```

```
uecccloud@UECserver01:~/.euca$ sudo euca_conf --list-nodes  
[sudo] password for uecccloud:  
registered nodes:  
  10.0.0.3  UECcluster01  
  10.0.0.4  UECcluster01
```

Scaling out the cloud – adding a whole cluster

Another scaling-out option would be adding a whole cluster. As mentioned in the main document, there are several possible reasons to do that: wanting to run different hypervisor, spreading clusters on several data centers, and having different clusters for different departments.

In our case, we will add a CC/SC creating another cluster, and we will add one node to that cluster afterwards.

Installation of fifth server (CC, SC)

The Cloud Controller and Storage Controller server would be configured as:

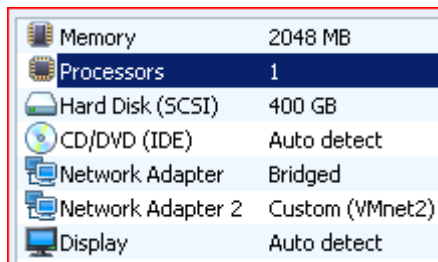
UECserver05

Roles: CC, SC

Processor architecture: 64 bit

VT: not necessarily VT enabled

Network: public (VMnet0), private (VMnet2)



Memory	2048 MB
Processors	1
Hard Disk (SCSI)	400 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Bridged
Network Adapter 2	Custom (VMnet2)
Display	Auto detect

Mount the installation media, and boot from it. Choose the language – English. Follow the same steps as installing other servers, until you reach to the point of configuring the network.

If your network is configured with DHCP, stop the process (ESC) and jump to the step of configuring your network manually. (The servers should be configured with static IP addresses)

Set up static IP for the (public) network interface:

IP address 192.168.1.97

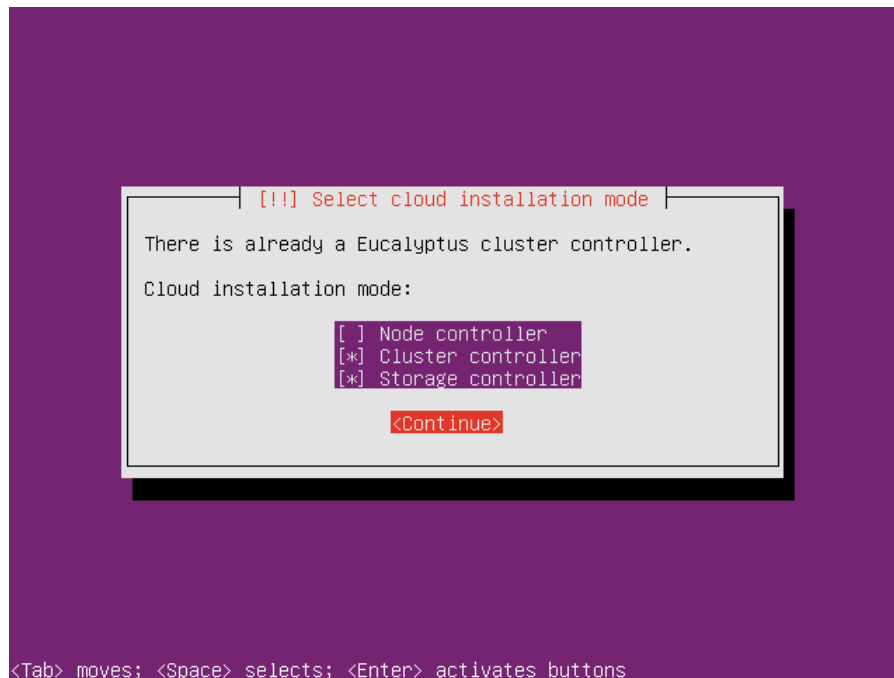
netmask 255.255.255.0

gateway 192.168.1.1

name server addresses: 192.168.1.99

Write “**UECserver05**” for the hostname. For the domain name, write “**UECcloud.private**”.

The installation can contact the CLC and get information that the CLC and WS3 components are installed in the cloud, and that there is already a cluster controller. Remove the Node Controller, and choose to install the CC and SC components:



Since we have two network interfaces in the system, we should designate one that is to be used for communication with computing nodes (NCs). Since our computing nodes are placed on the private network, we should choose the secondary network interface (eth1) as the one used for communicating with nodes.

Configuring disks is done by following the same procedure as for the first server. Installing of the base system starts, after that the configuring of the APT, then installing the software.

The installation reaches the point of configuring the cluster. Name the cluster as "UECcluster02", since we already have one cluster. Add the following pool of IP addresses: 192.168.1.200-192.168.1.250: (We are not taking the whole class C subnet, since we used the previous range for the first cluster)



After the successful installation, the server reboots.

Post installation steps

As a first step, check the configuration of the network interfaces, and set up static IP for the private network interface (eth1):

```
sudo vi /etc/network/interfaces
```

Add the following:

```
auto eth1  
iface eth1 inet static  
    address 10.0.0.5  
    netmask 255.255.255.0  
    network 10.0.0.0  
    broadcast 10.0.0.255
```

Restart the networking to apply the changes:

```
sudo /etc/init.d/networking restart
```

To be able to synchronize the time on the server, we will install NTP:

```
sudo apt-get install ntp
```

*(if error "unable to locate package" occurs, run **sudo apt-get update**)*

To make the server synchronize the time with the first server, open the file **/etc/ntp.conf** and add:

```
server 10.0.0.1
```

Restart the NTP service afterwards to make the changes effective:

```
sudo /etc/init.d/ntp restart
```

Check server time:

```
date
```

Check the DNS configuration **/etc/resolv.conf** - it should look like:

```
search UECcloud.private  
nameserver 10.0.0.1
```

Make sure that you have the latest version of Eucalyptus:

```
sudo apt-get upgrade eucalyptus
```

This is the last step of initial configuration for the second server in the cloud, and to make sure that the configuration is implemented, restart the machine (**sudo reboot**) and eventually check the installed features.

Now that we added the cluster, we can see it:

```
euca-describe-availability-zones
```

```
ueccloud@UECserver01:~/.euca$ euca-describe-availability-zones  
AVAILABILITYZONE      UECcluster01      192.168.1.98  
AVAILABILITYZONE      UECcluster02      192.168.1.97
```

Installation of sixth server (NC)

The Node Controller server, that is going to be added to our second cluster, would be configured as:

UECserver06

Roles: NC

Processor architecture: 64 bit

VT: VT enabled

Network: private (VMnet2)

Memory	4096 MB
Processors	2
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using drive D:
Network Adapter	Custom (VMnet2)
Display	Auto detect

Mount the installation media, and boot from it. Choose the language – English. Follow the same steps as installing other servers, until you reach to the point of configuring the network. Choose to configure the network manually.

Set up static IP for the (private) network interface.

IP address 10.0.0.6

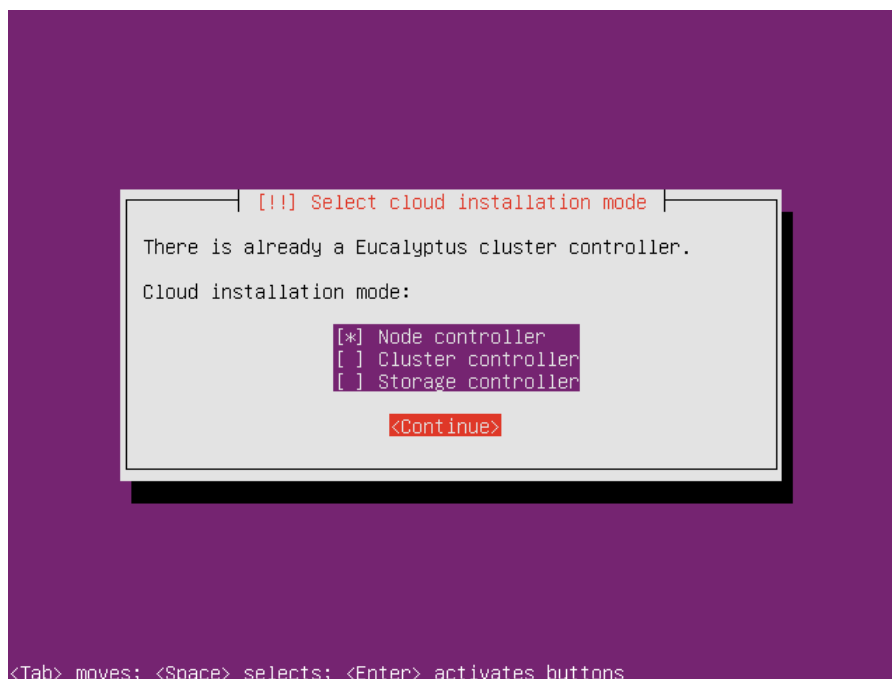
netmask 255.255.255.0

gateway 10.0.0.1

name server addresses: 10.0.0.1

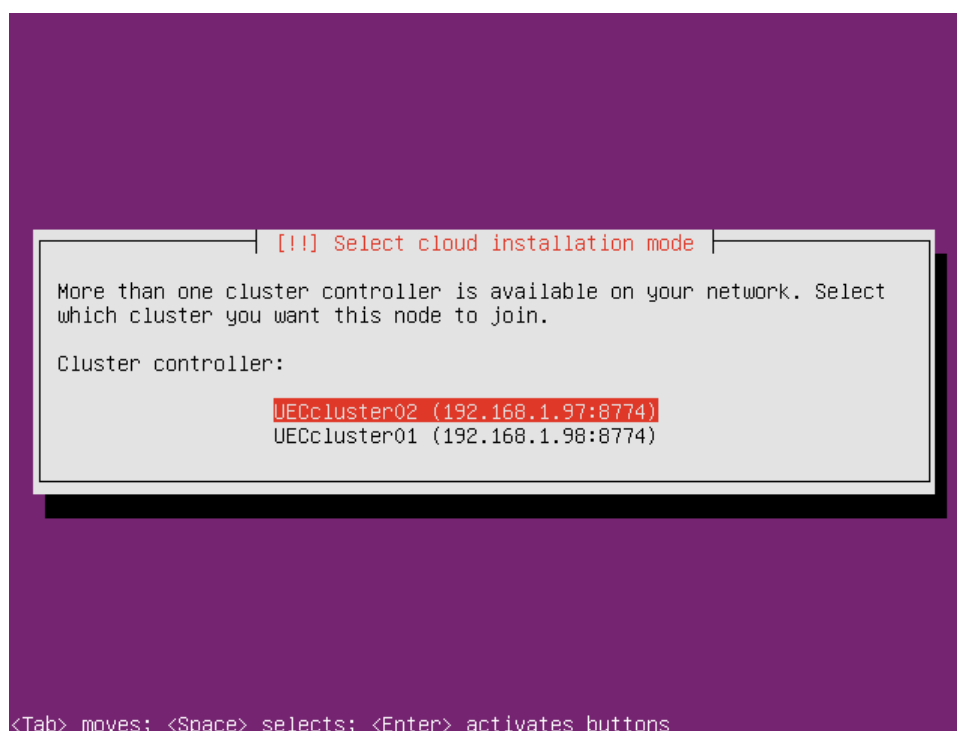
Write “UECserver06” for the hostname. For the domain name, write “UECcloud.private”.

The installation can contact the CLC and get information about CLC, WS3, CC and SC components are installed in the cloud, and offer to install the NC component on the server:



Choose to install a NC.

Now, we have to choose the cluster which the NC will be installed under. We want the NC to belong to the second cluster we just created, "UECcluster02":



Configuring disks is done by following the same procedure as for the first server. Installing of the base system starts, after that the configuring of the APT, then installing the software.

Again, if you get the error about hardware not supporting virtualization acceleration, please check if your processor is VT-enabled (having VT extensions), and remember to turn that option on in BIOS.

(In our case, we get the error since we are installing UEC inside a virtual machine, where VT extensions are not supported)

After the successful installation, the server reboots.

Post installation steps

As a first step, check the configuration of the network interface (eth0):

sudo vi /etc/network/interfaces

(Networking is implemented using bridging.)

To check network connectivity, try pinging an address that you positively know is giving response to ping requests.

To be able to synchronize the time on the server, install NTP:

sudo apt-get install ntp

(if error "unable to locate package" occurs, run **sudo apt-get update**)

To make the server synchronize the time with the first server, open the file **/etc/ntp.conf** and add:

server 10.0.0.1

Restart the NTP service afterwards to make the changes effective:

sudo /etc/init.d/ntp restart

Check server time:
date

Check the DNS configuration **/etc/resolv.conf** - it should look like:
search UECcloud.private
nameserver 10.0.0.1

Make sure that you have the latest version of Eucalyptus:
sudo apt-get upgrade eucalyptus

Restart the NC:
sudo restart eucalyptus-nc

This is the last step of initial configuration for the third server in the cloud, and to make sure that the configuration is implemented, restart the machine (**sudo reboot**) and eventually check the installed features.

Verifying the cloud after the scale-out

The clusters present in the cloud are our two clusters:
euca-describe-availability-zones

```
uecccloud@UECserver01:~/.euca$ euca-describe-availability-zones
AVAILABILITYZONE    UECcluster01    192.168.1.98
AVAILABILITYZONE    UECcluster02    192.168.1.97
```

The nodes present in the cloud are the three nodes, two belonging to first cluster, and one belonging to second cluster:

sudo euca_conf --list-nodes

```
uecccloud@UECserver01:~/.euca$ sudo euca_conf --list-nodes
[sudo] password for uecccloud:
registered nodes:
  10.0.0.3  UECcluster01
  10.0.0.4  UECcluster01
  10.0.0.6  UECcluster02
```

In the cloud's web interface, both clusters are present in the configuration:

Clusters:

Name: UECcluster02 Deregister Cluster

Cluster Controller

Host: 192.168.1.97

☒ Dynamic public IP address assignment

Reserve for assignment 10 public IP addresses

Maximum of 5 public IP addresses per user

Use VLAN tags 10 through 4095

Storage Controller

Name: UECcluster01 Deregister Cluster

Cluster Controller

Host: 192.168.1.98

☒ Dynamic public IP address assignment

Reserve for assignment 10 public IP addresses


Maximum of 5 public IP addresses per user

Use VLAN tags 10 through 4095







Storage Controller

Register cluster Save cluster configuration Clusters up to date

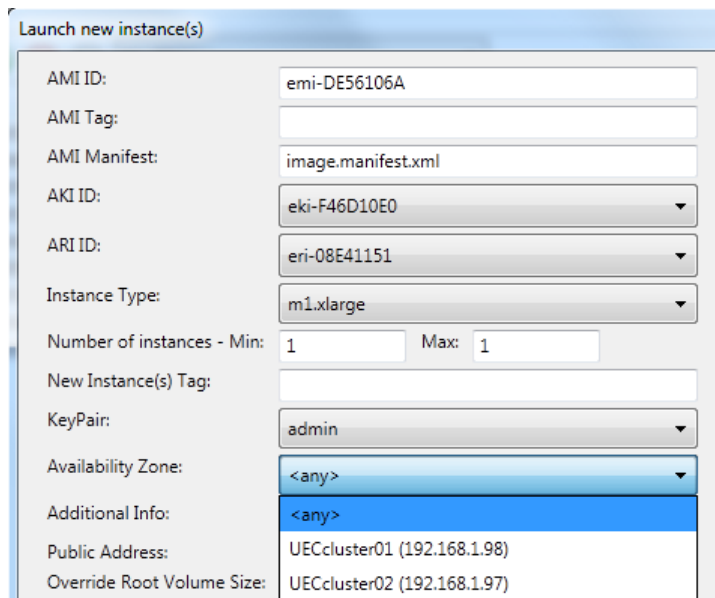
In HybridFox we can see both of the clusters under the availability zones:

Availability Zones	
	
Name	State
UECcluster01	192.168.1.98
UECcluster02	192.168.1.97

Under Elastic IPs, we can see that the IP address pool is now comprised of the pools of the two clusters:

Your Elastic IPs	
     	
Address	Instance ID
192.168.1.196	nobody
192.168.1.197	nobody
192.168.1.198	nobody
192.168.1.199	nobody
192.168.1.200	nobody
192.168.1.201	nobody
192.168.1.202	nobody
192.168.1.203	nobody
192.168.1.204	nobody
192.168.1.205	nobody
192.168.1.206	nobody
192.168.1.207	nobody

Launching an instance, we can now choose on which cluster we would like the instance to run:



AMI ID:	emi-DE56106A		
AMI Tag:			
AMI Manifest:	image.manifest.xml		
AKI ID:	eki-F46D10E0		
ARI ID:	eri-08E41151		
Instance Type:	m1.xlarge		
Number of instances - Min:	1	Max:	1
New Instance(s) Tag:			
KeyPair:	admin		
Availability Zone:	<any>		
Additional Info:	<any>		
Public Address:	UECcluster01 (192.168.1.98)		
Override Root Volume Size:	UECcluster02 (192.168.1.97)		

Acknowledgement

The work reported in this report has been partially funded by the Danish Agency for Science, Technology and Innovation under the project "Next Generation Technology for Global Software Development", #10-092313.