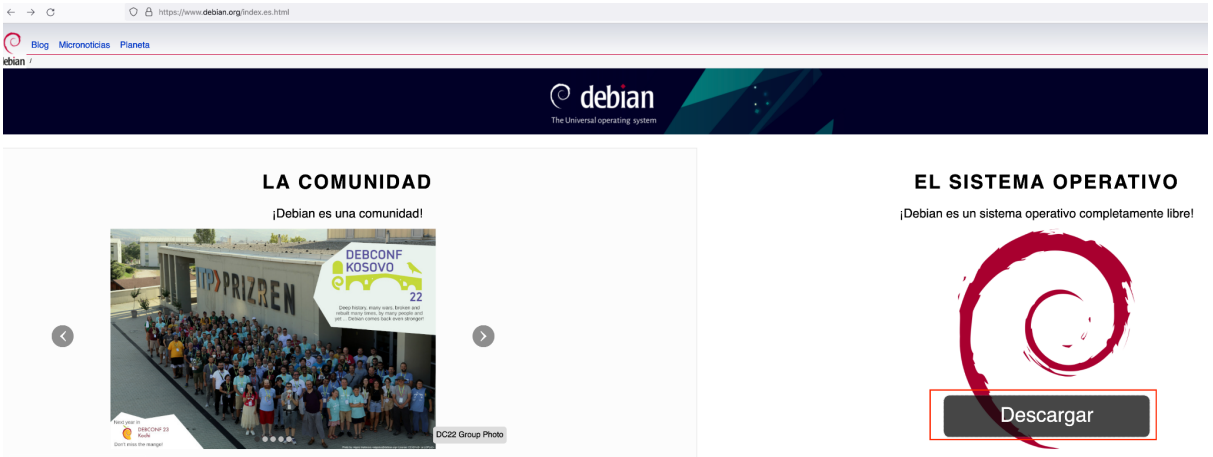
Born2Beroot

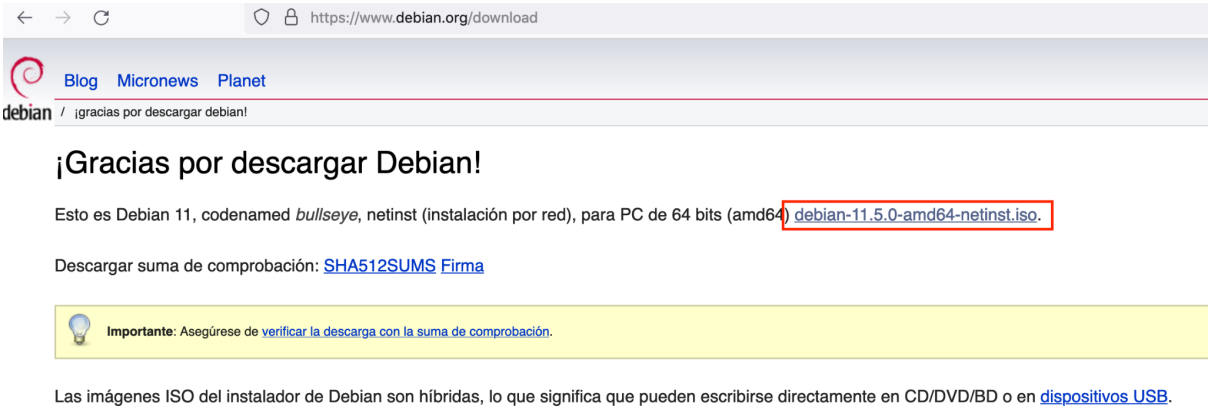
sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus

1. Install Debian

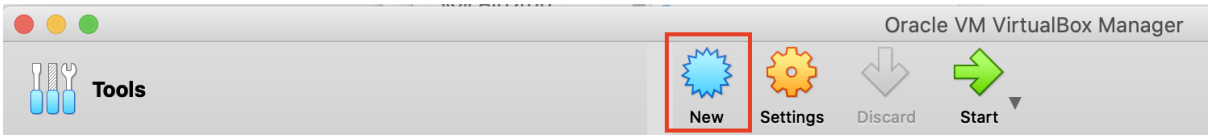
First, go to https://www.debian.org and download the last version of Debian.



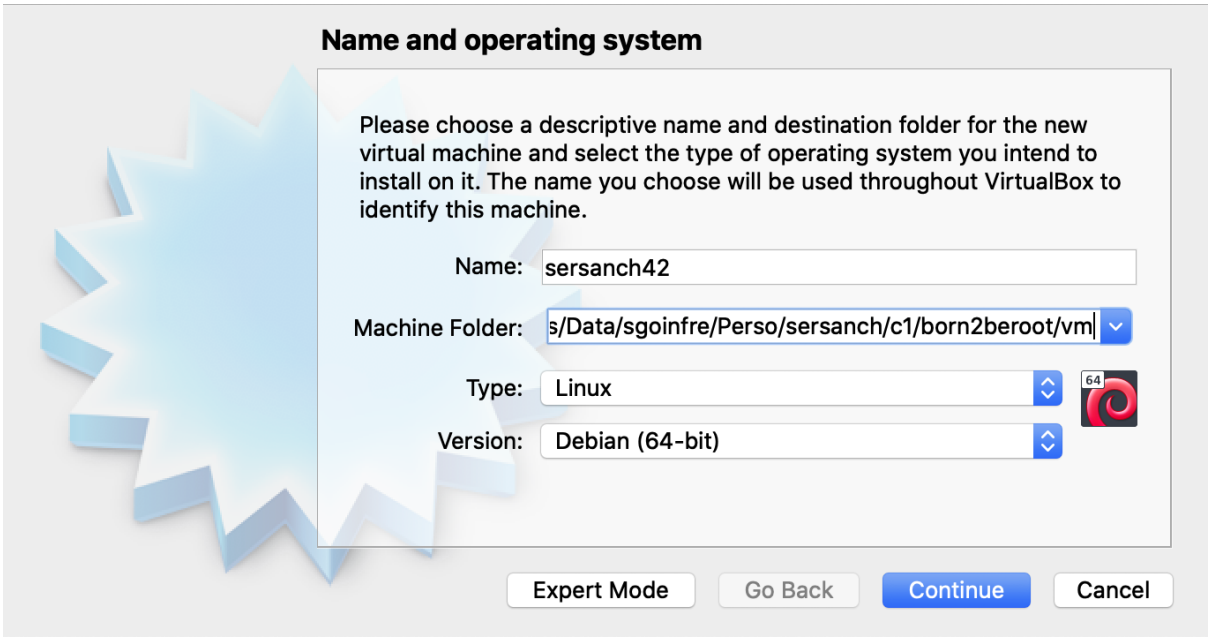
You can download it from the following link.



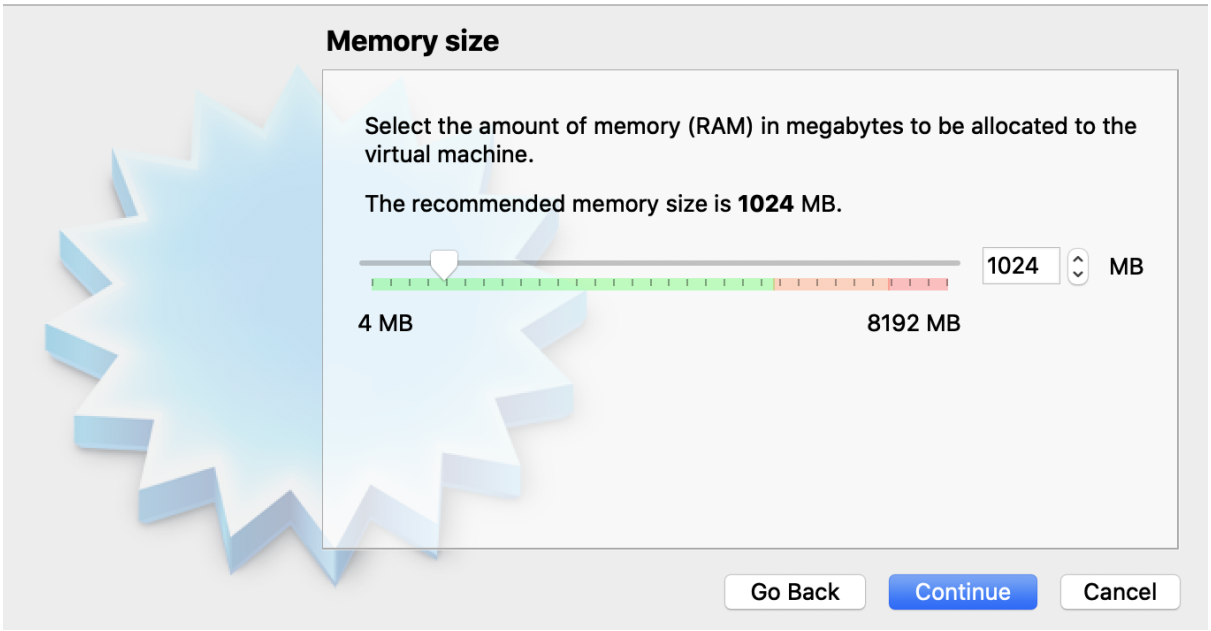
Next, open VirtualBox and click on the “New” button.



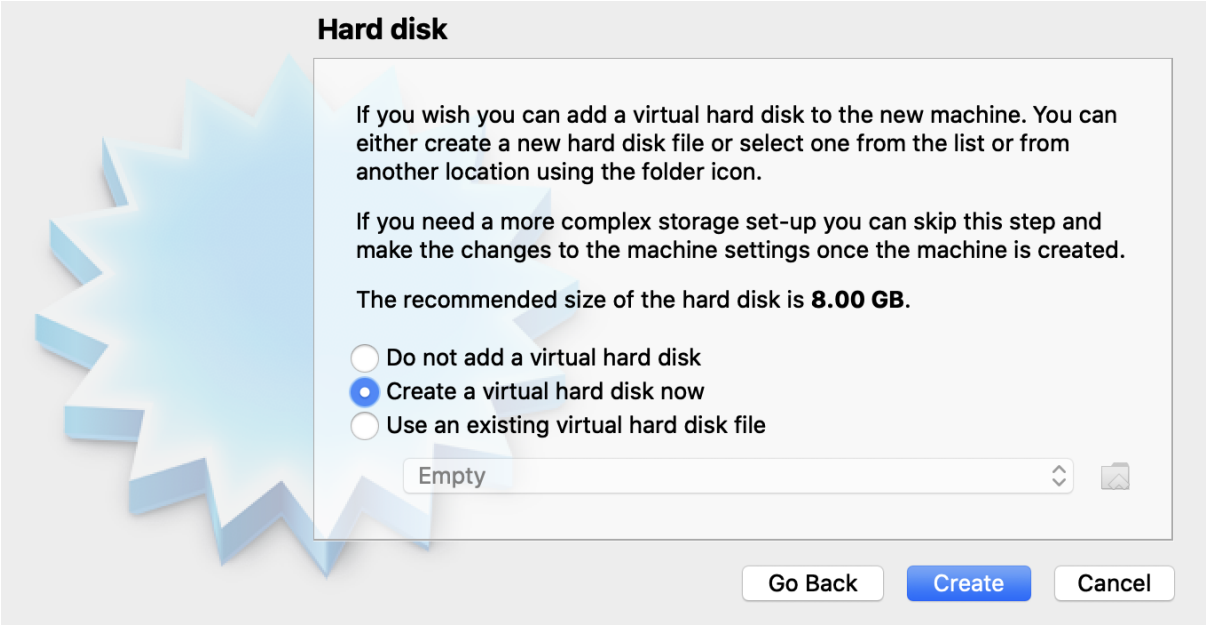
I’ve chosen “sersanch42” for my instance and a custom folder for store the virtual machine. Select Linux and Debian (64-bit in my case).



Leave the default memory. If you assign more memory, try to be below the orange bar.

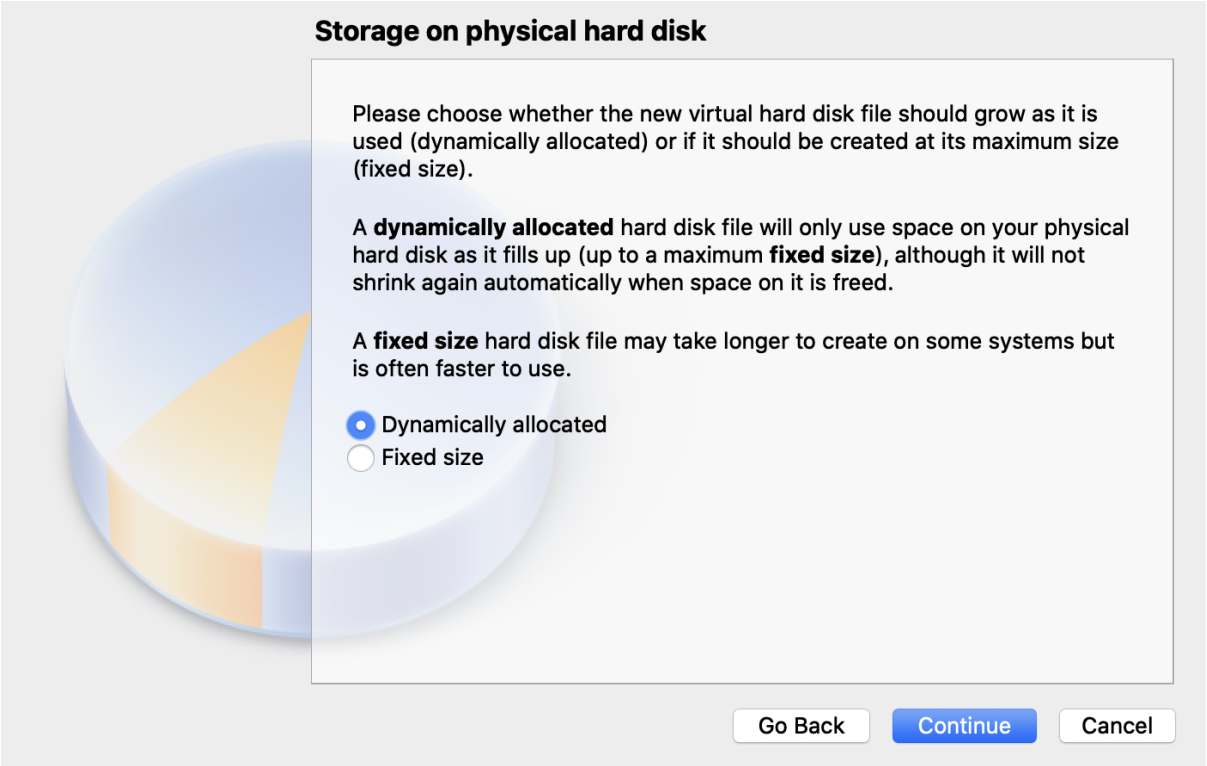


Select the option for creating a new virtual hard disk.

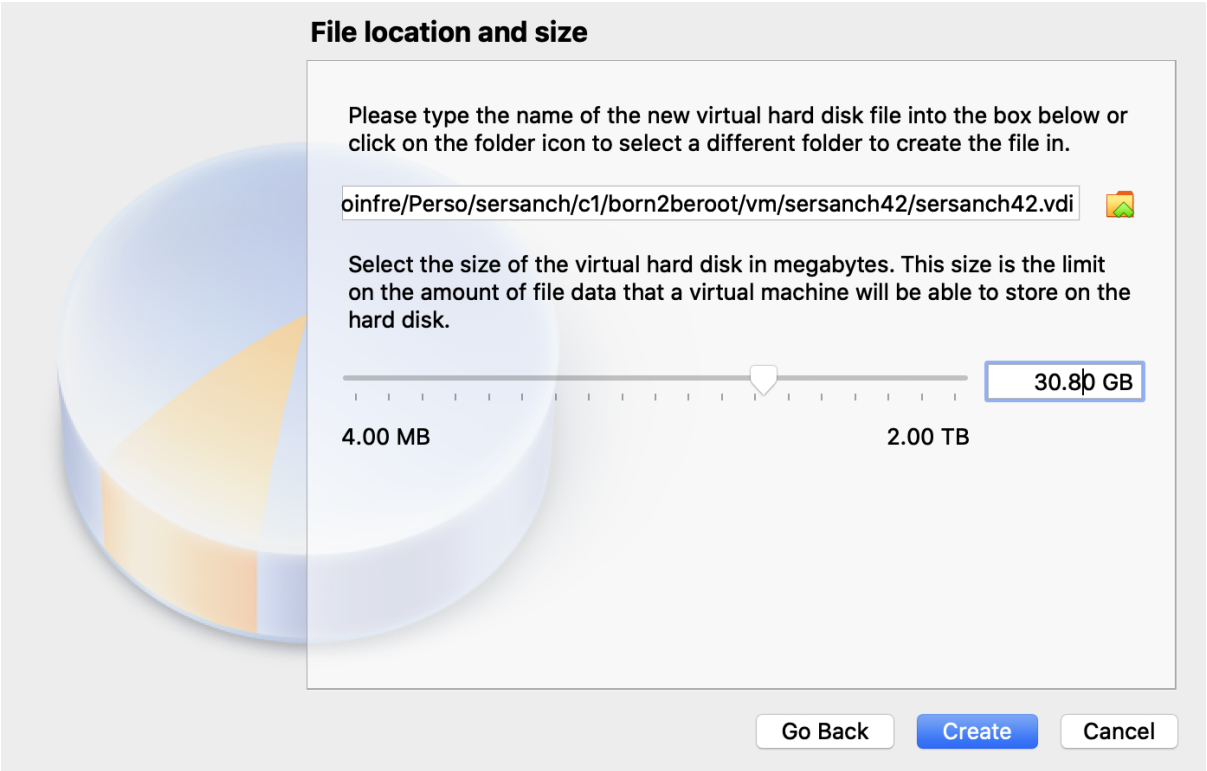


There are three types of hard disk. Select VDI.

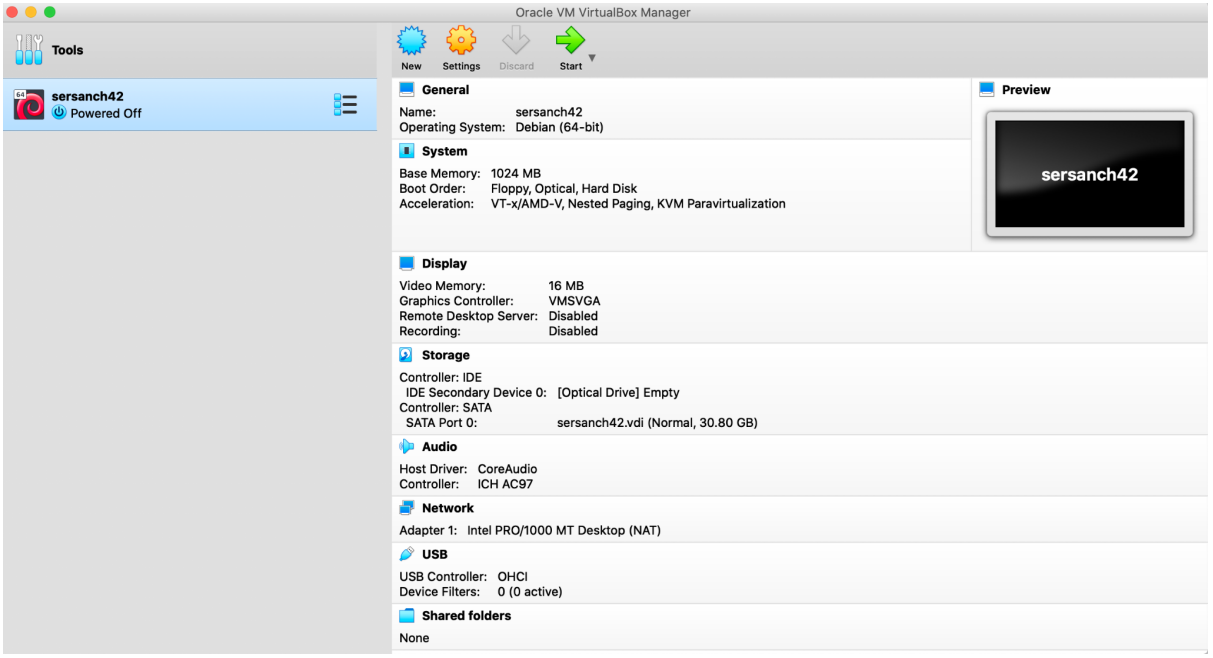
We don’t want to save the exact space for our VDI, so dynamically allocated memory is the best option. It will only use the space that the VM needs.



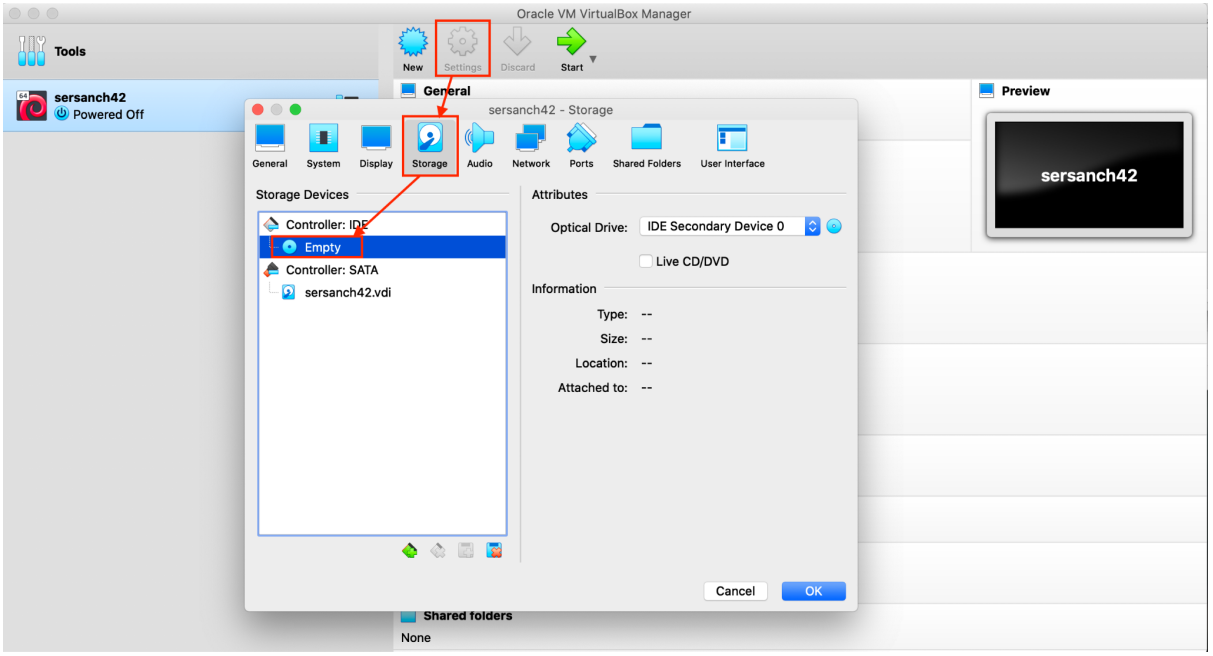
The folder where the VDI will be saved is inside the folder of the VM. The subjects tells us that we need a total memory of 30.8GB so that's the value we put inside the box.



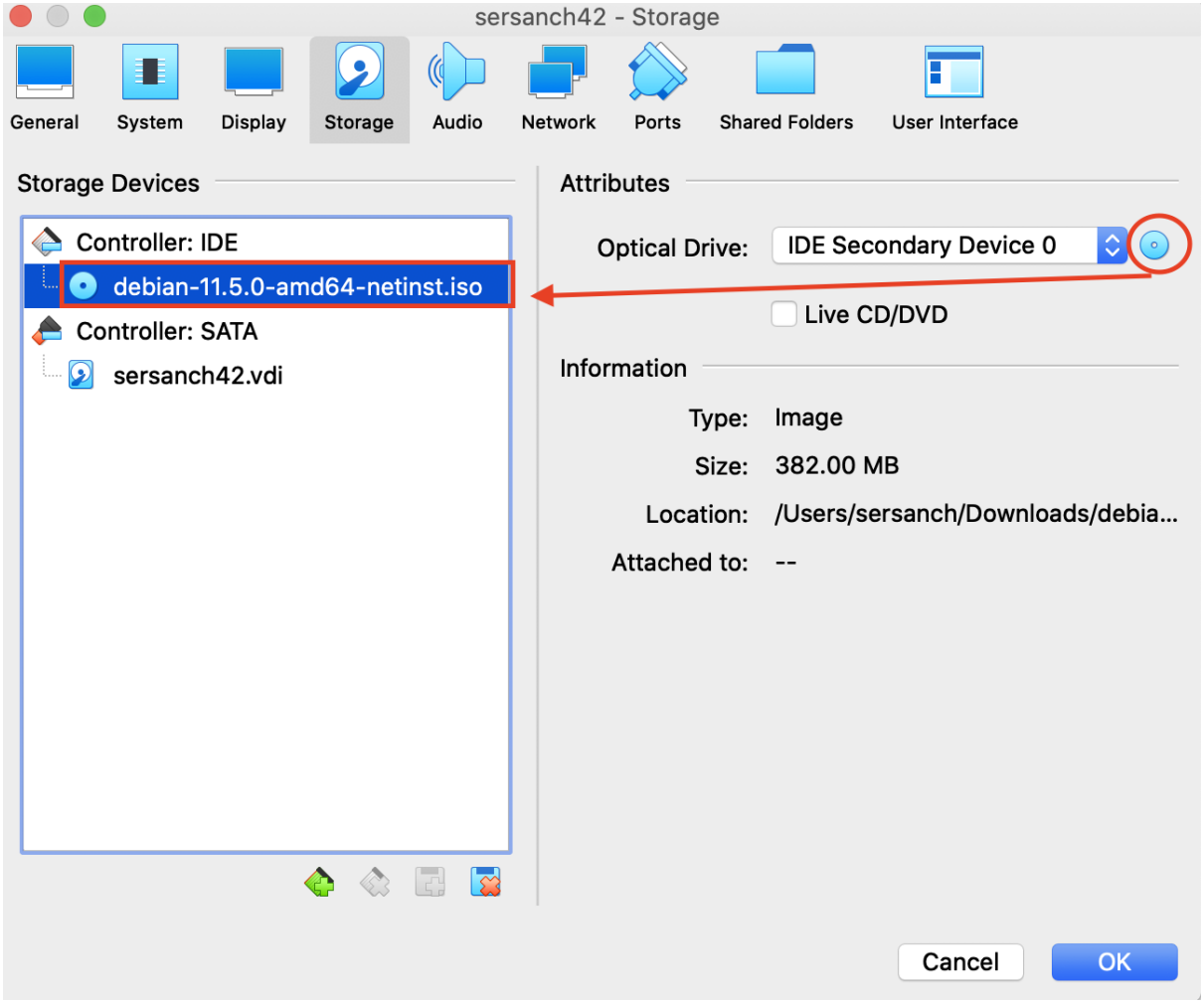
Now we have the new Debian VM ready for install.



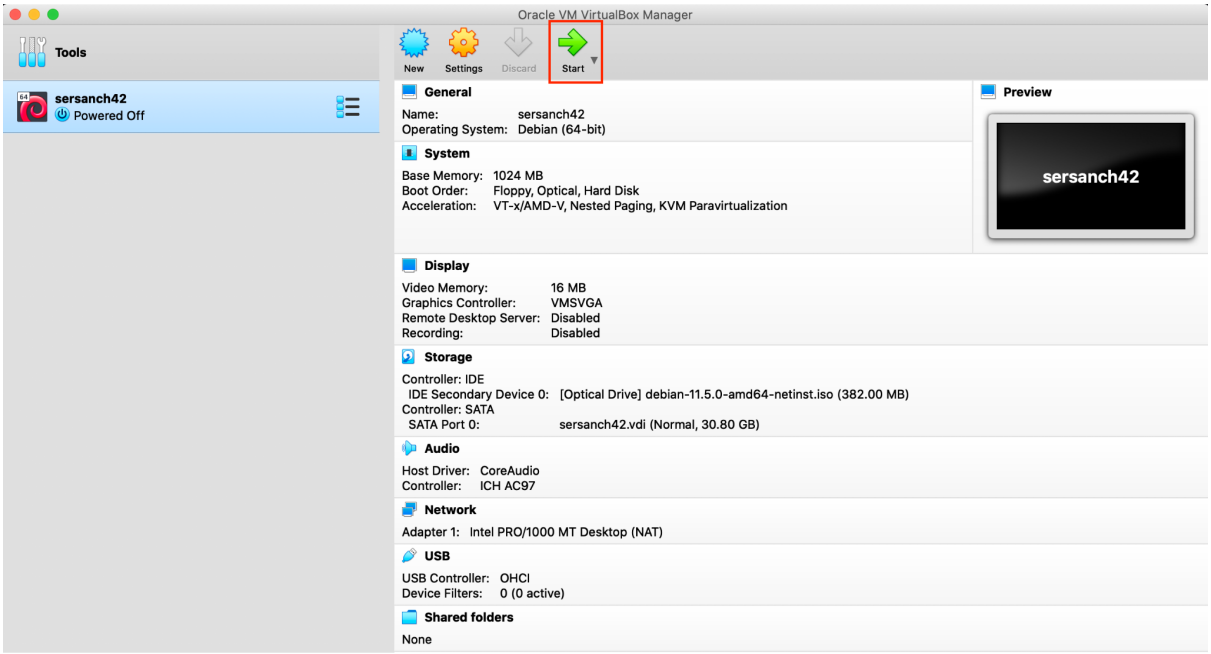
Go to “Settings” > “Storage” > click on the disc (“Empty”).



Click on the CD symbol at the right part of the screen and select the “.iso” file of Debian that we downloaded before.

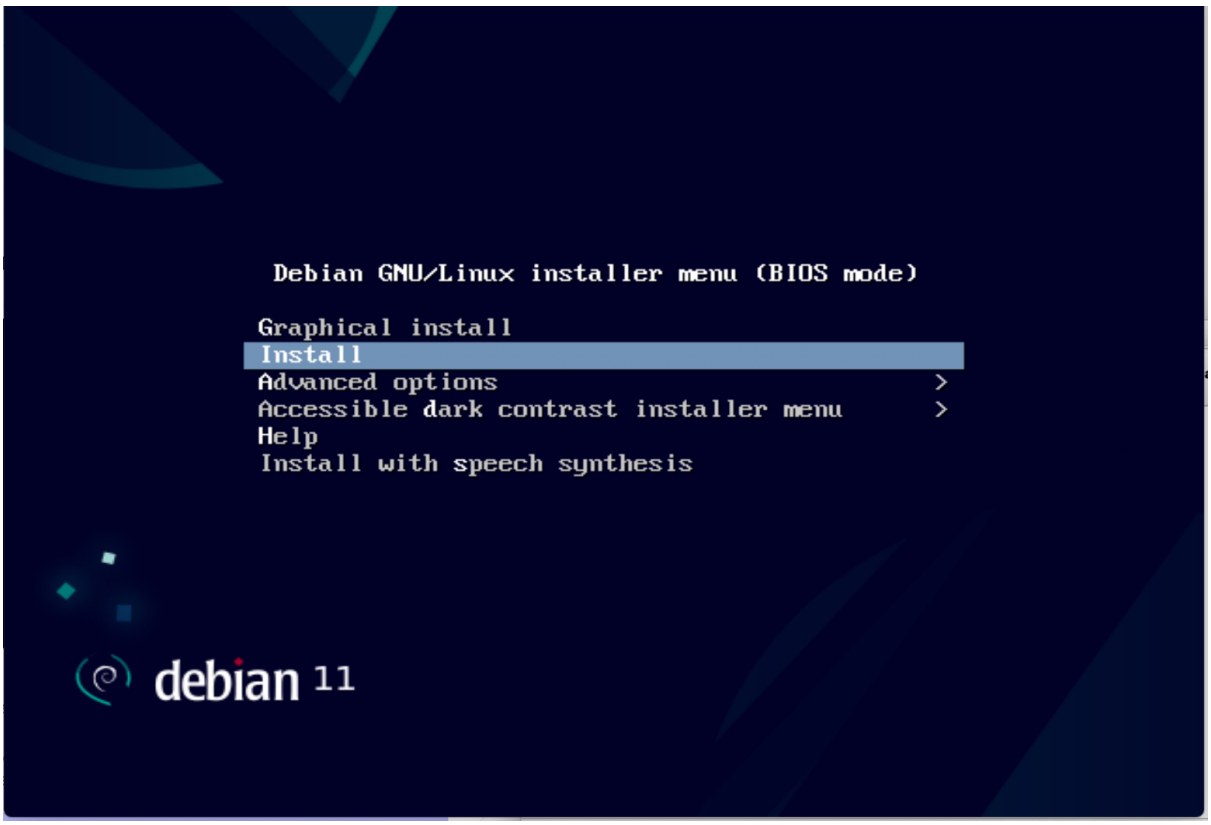


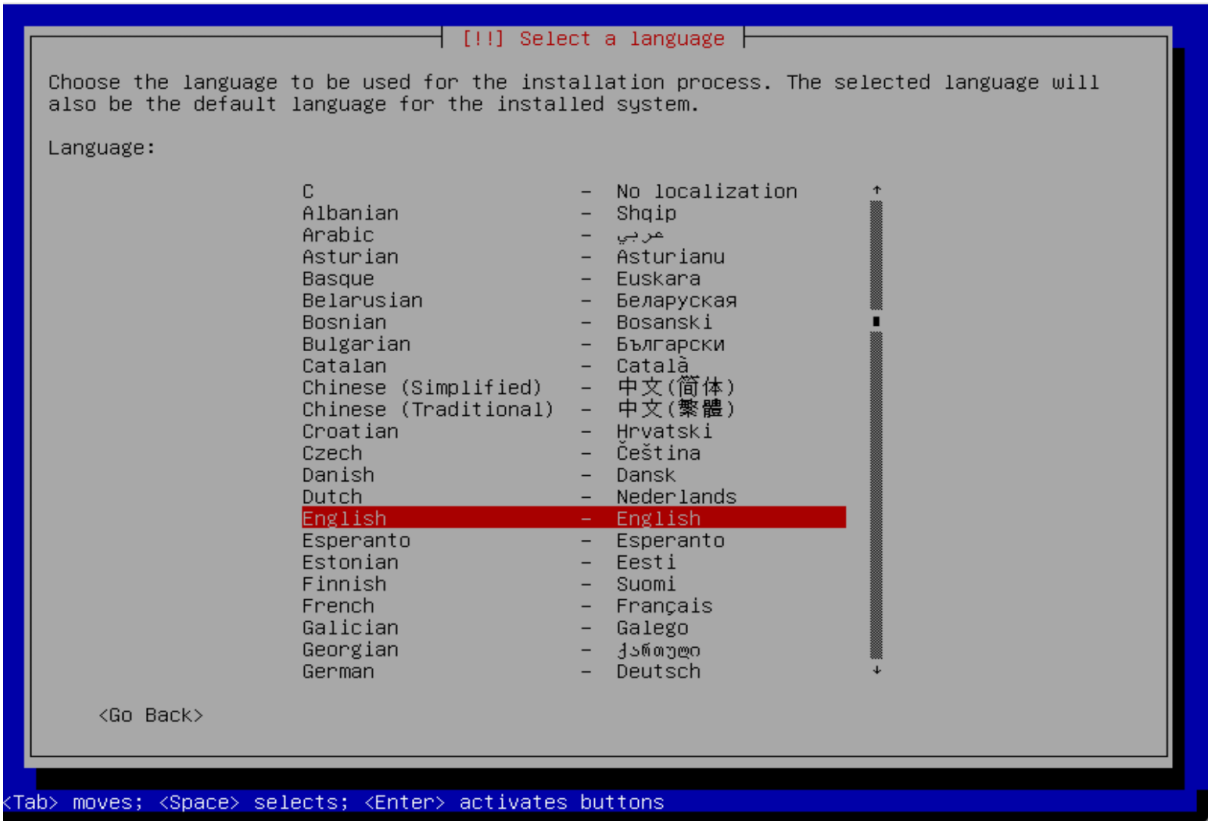
Now, start the machine clicking on the following symbol.

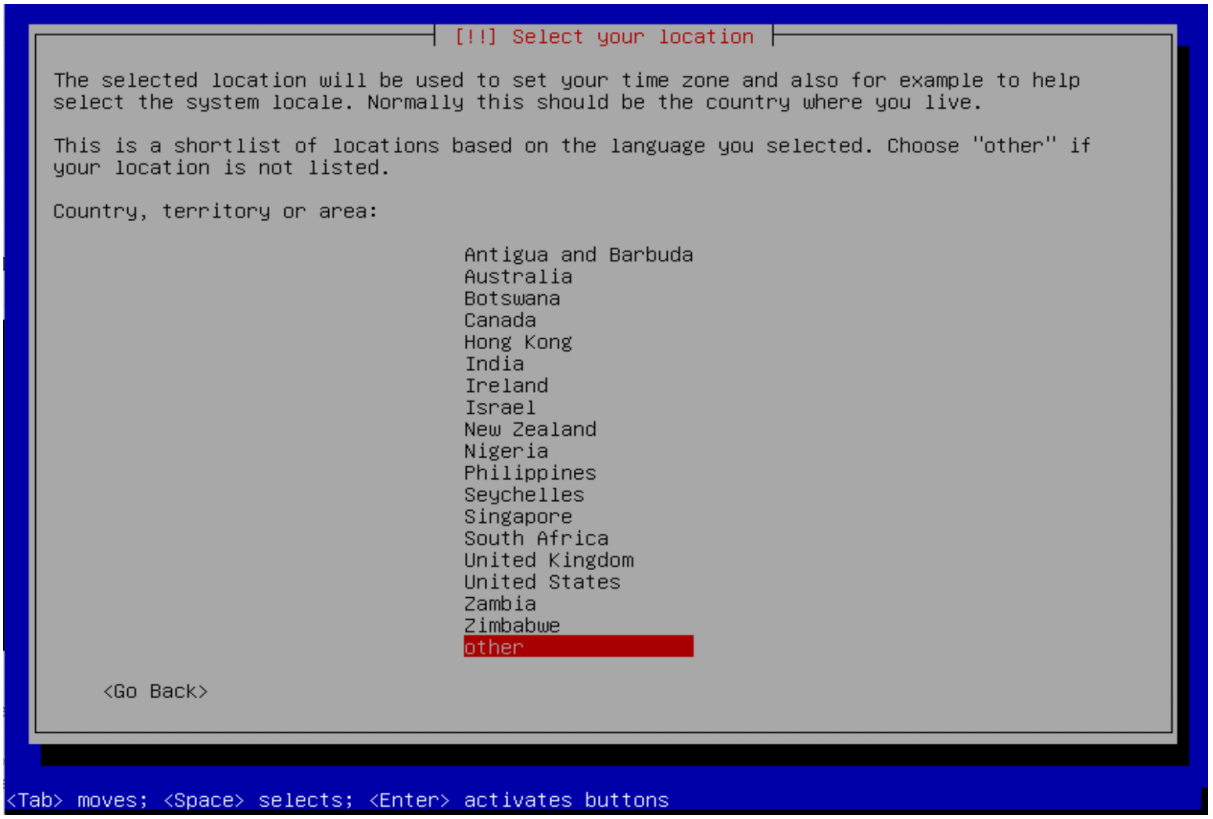


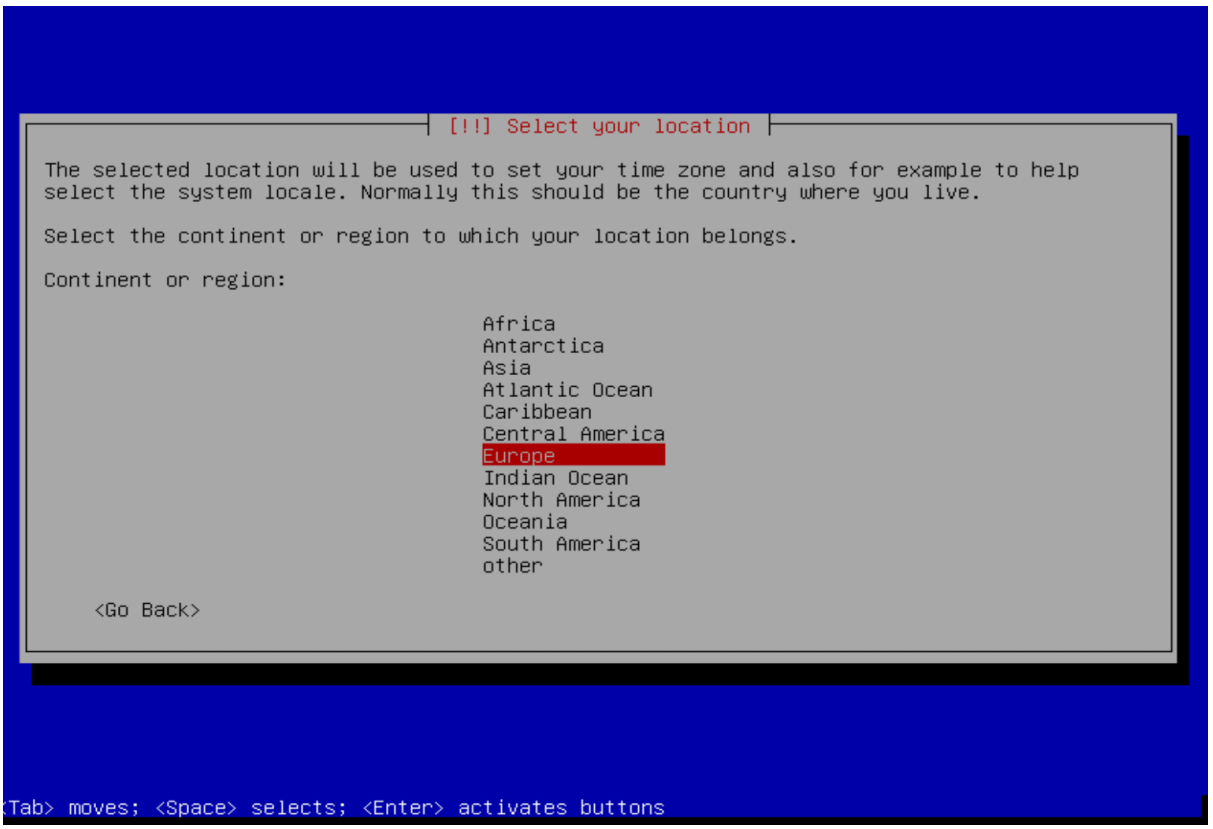
Follow the step in each screenshot.

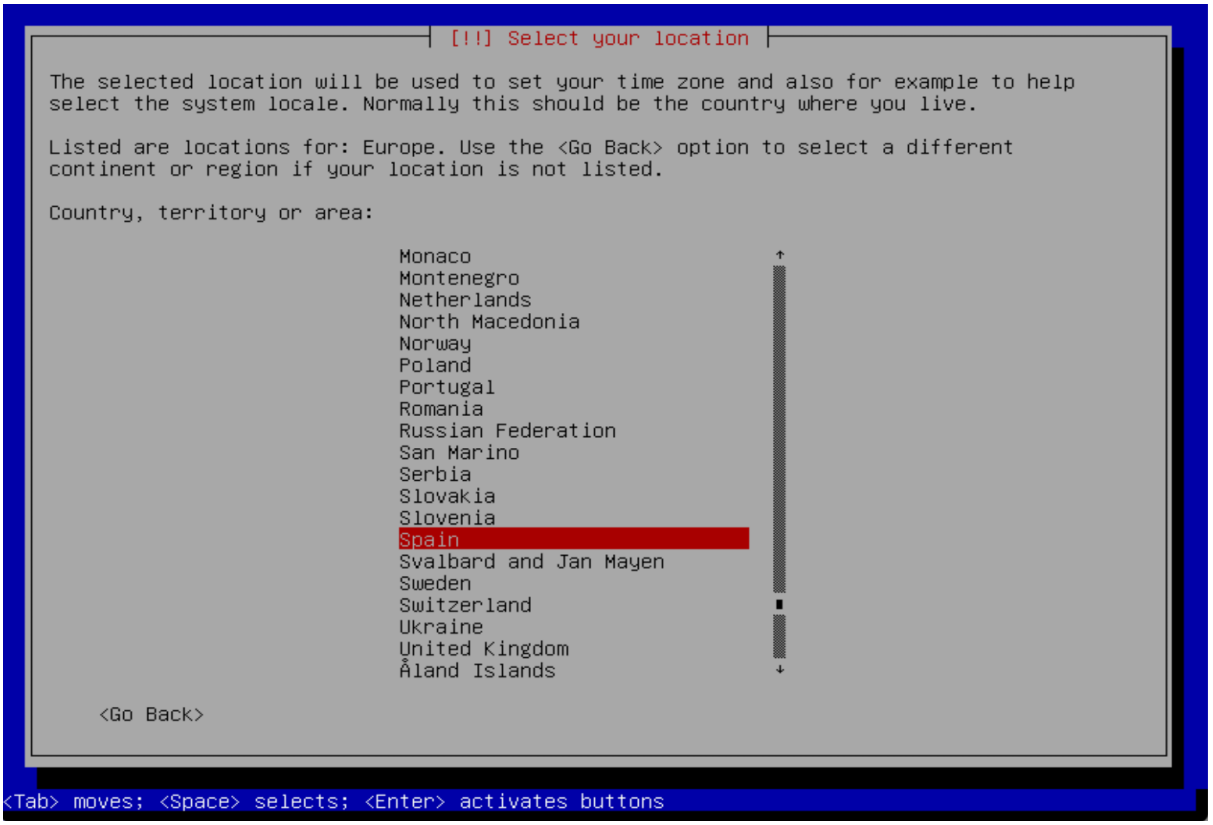
sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus

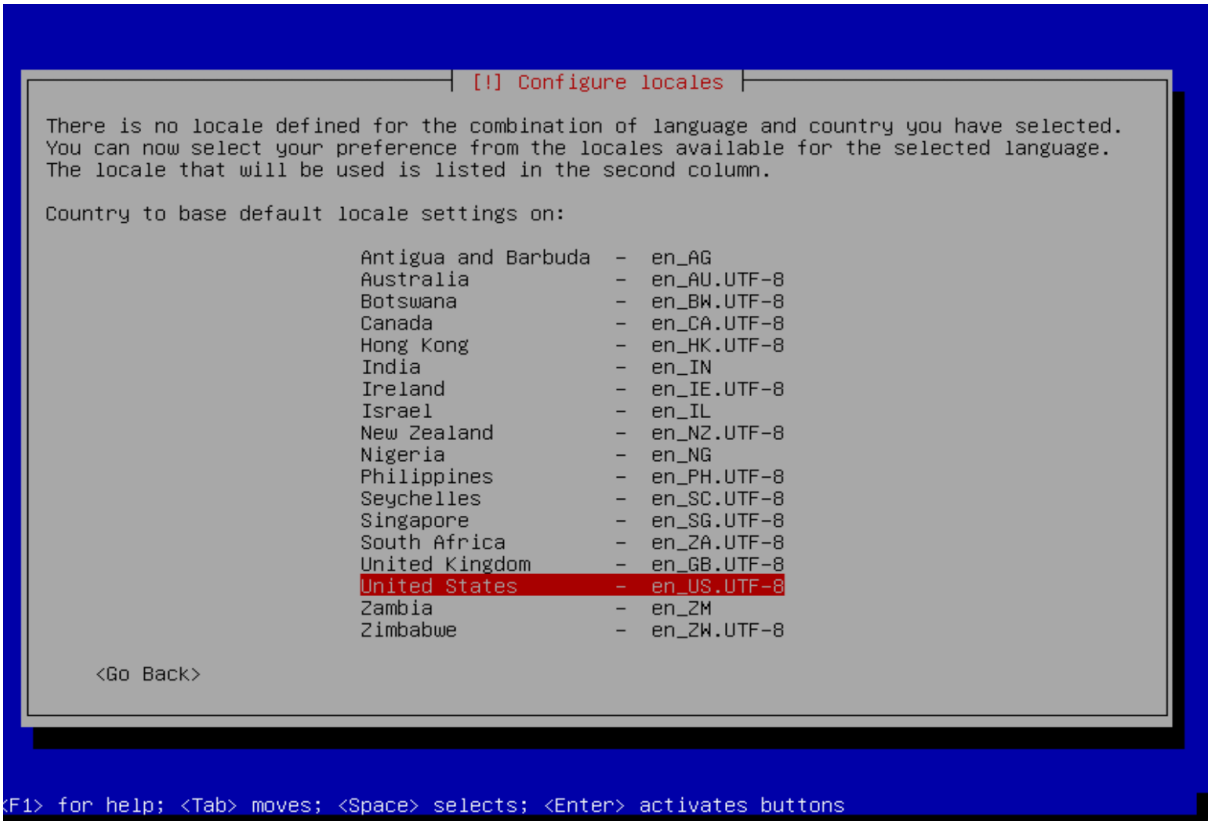

Debian GNU/Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options >
Accessible dark contrast installer menu >
Help
Install with speech synthesis
debian 11

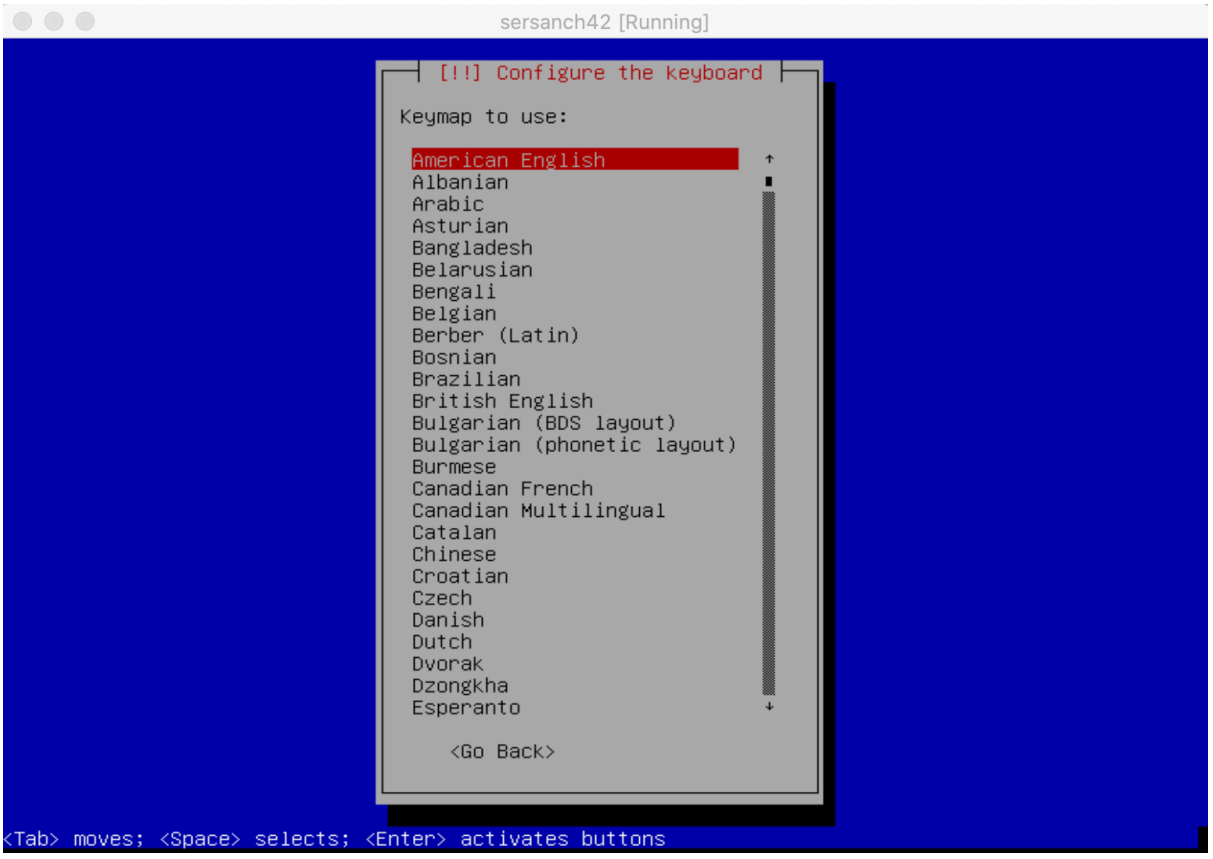

[!!] Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
C - No localization
Albanian - Shqip
Arabic - عربي
Asturian - Asturianu
Basque - Euskara
Belarusian - Беларуская
Bosnian - Bosanski
Bulgarian - Български
Catalan - Català
Chinese (Simplified) - 中文(简体)
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian - ქართული
German - Deutsch
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] 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.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
Antigua and Barbuda
Australia
Botswana
Canada
Hong Kong
India
Ireland
Israel
New Zealand
Nigeria
Philippines
Seychelles
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] 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

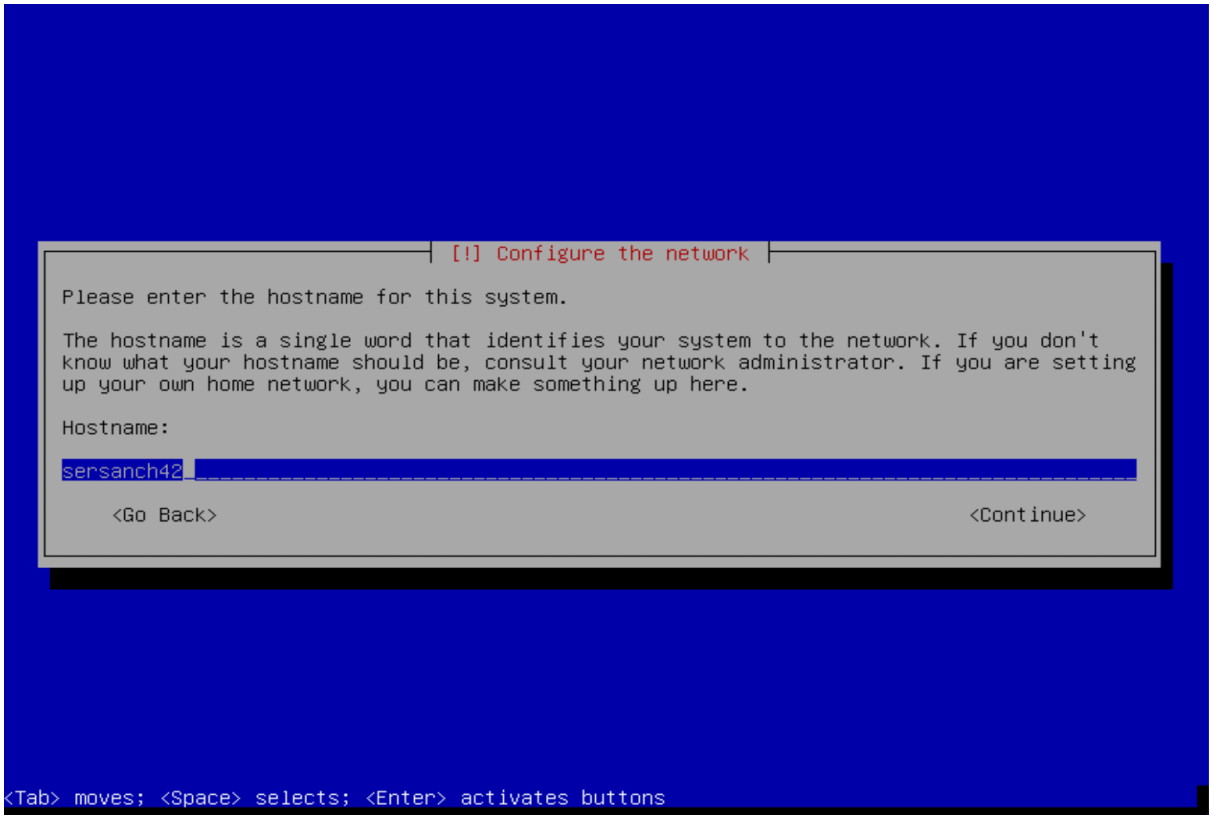

[!!] Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
Listed are locations for: Europe. Use the <Go Back> option to select a different continent or region if your location is not listed.
Country, territory or area:
Monaco
Montenegro
Netherlands
North Macedonia
Norway
Poland
Portugal
Romania
Russian Federation
San Marino
Serbia
Slovakia
Slovenia
Spain
Svalbard and Jan Mayen
Sweden
Switzerland
Ukraine
United Kingdom
Åland Islands
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons



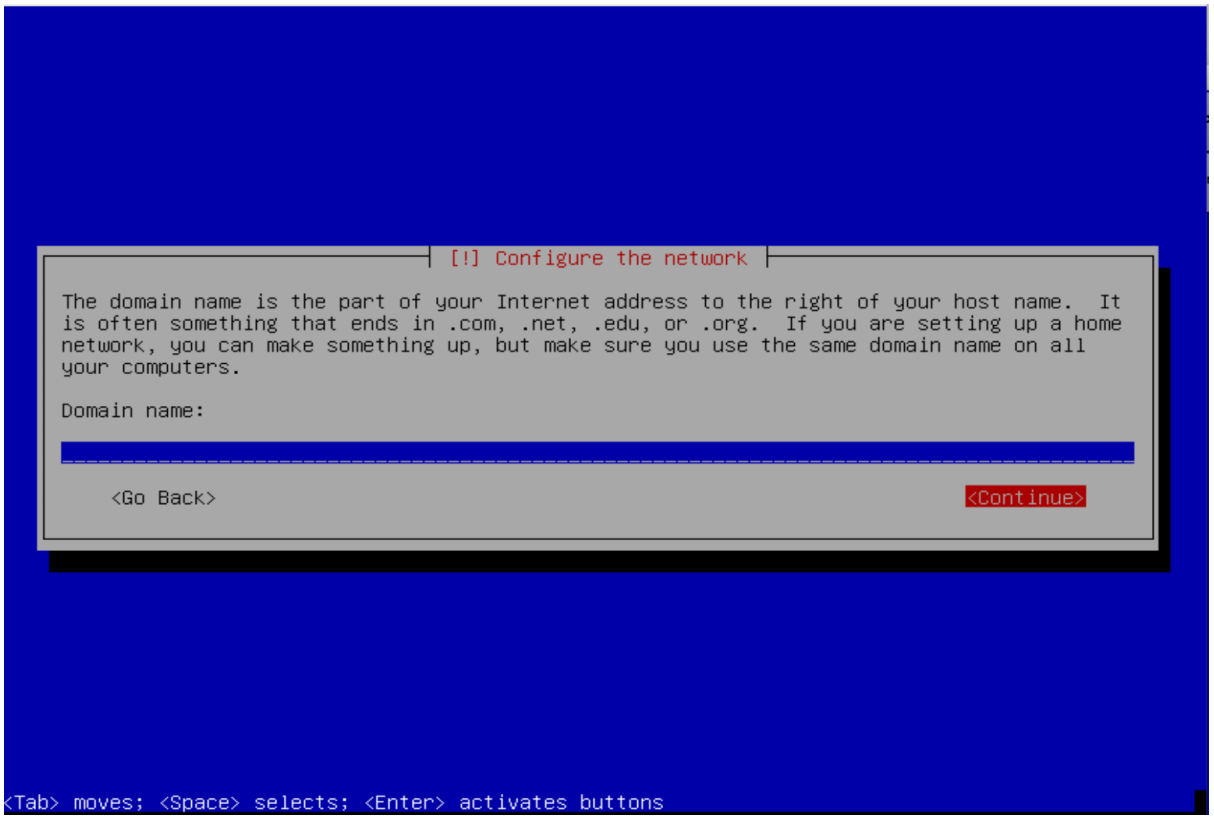


The installation requires that we name the hostname. The subject requires that the hostname must be our login ended with 42.

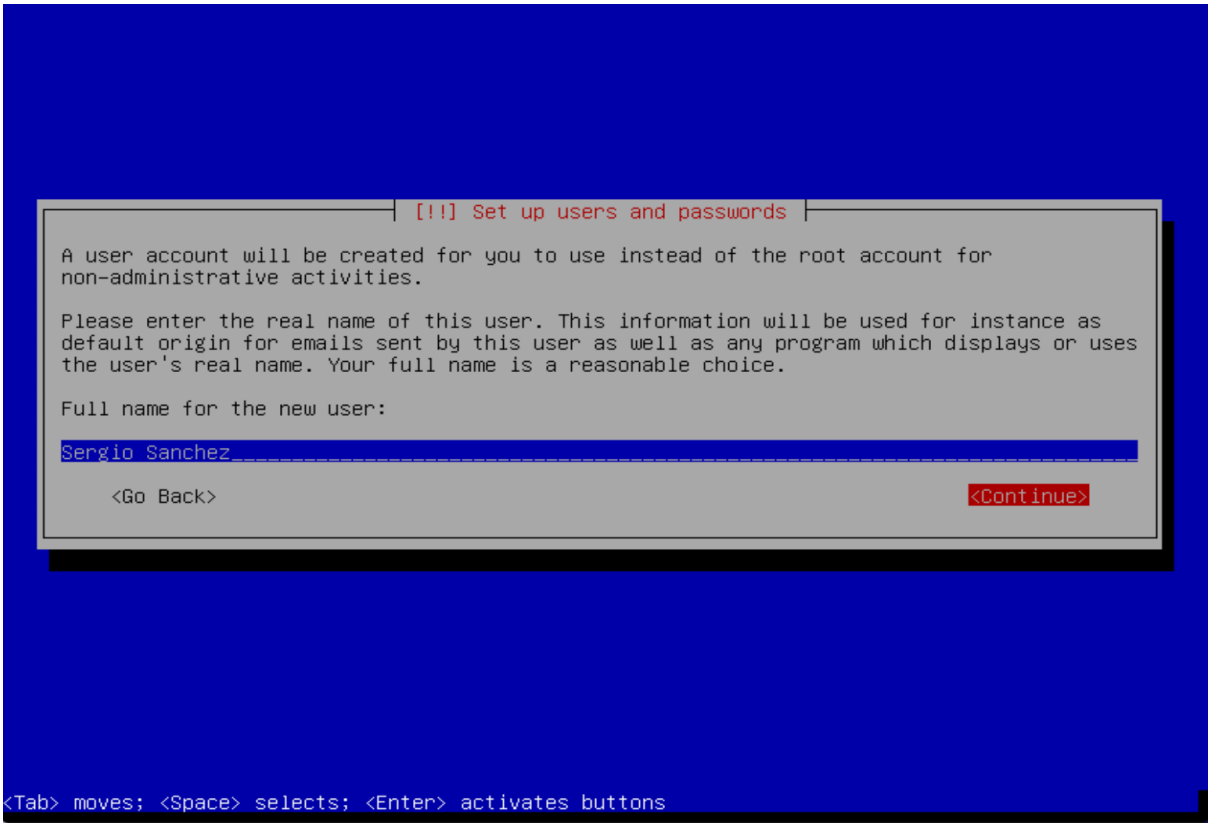
sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus

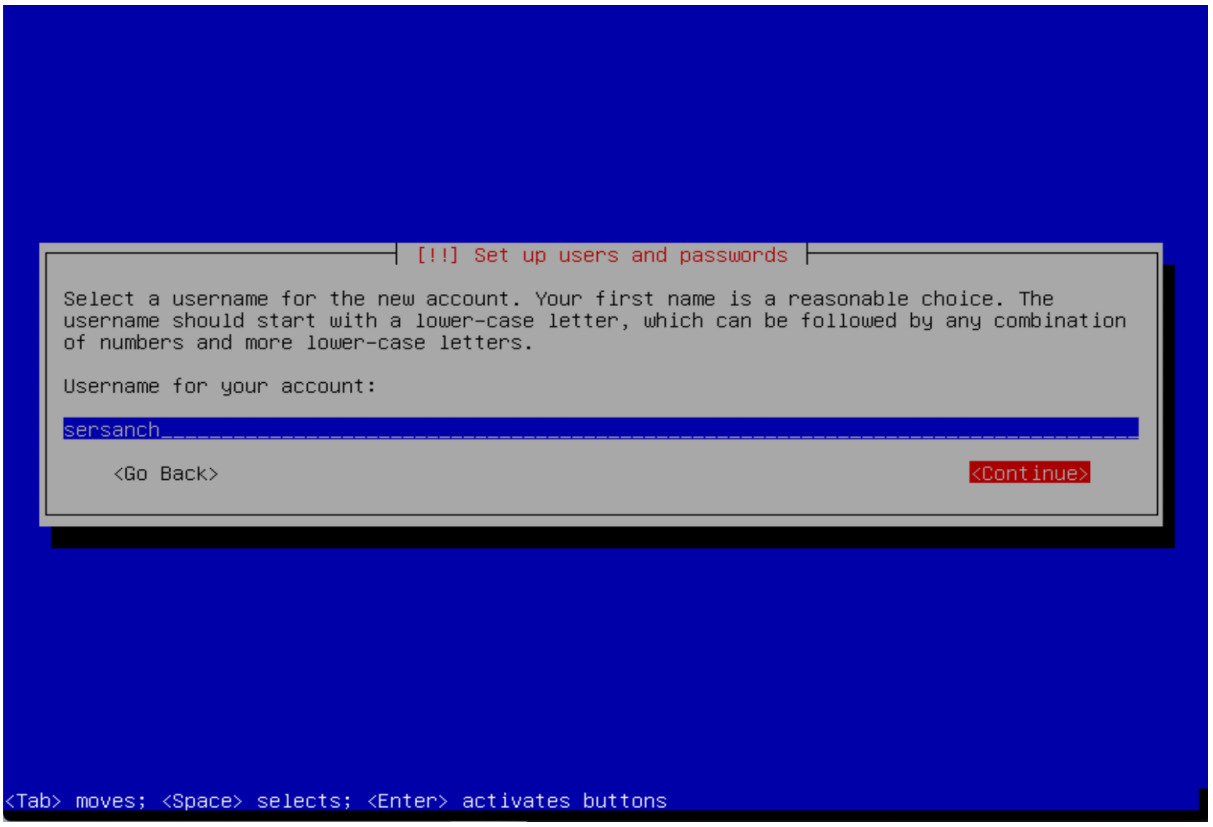


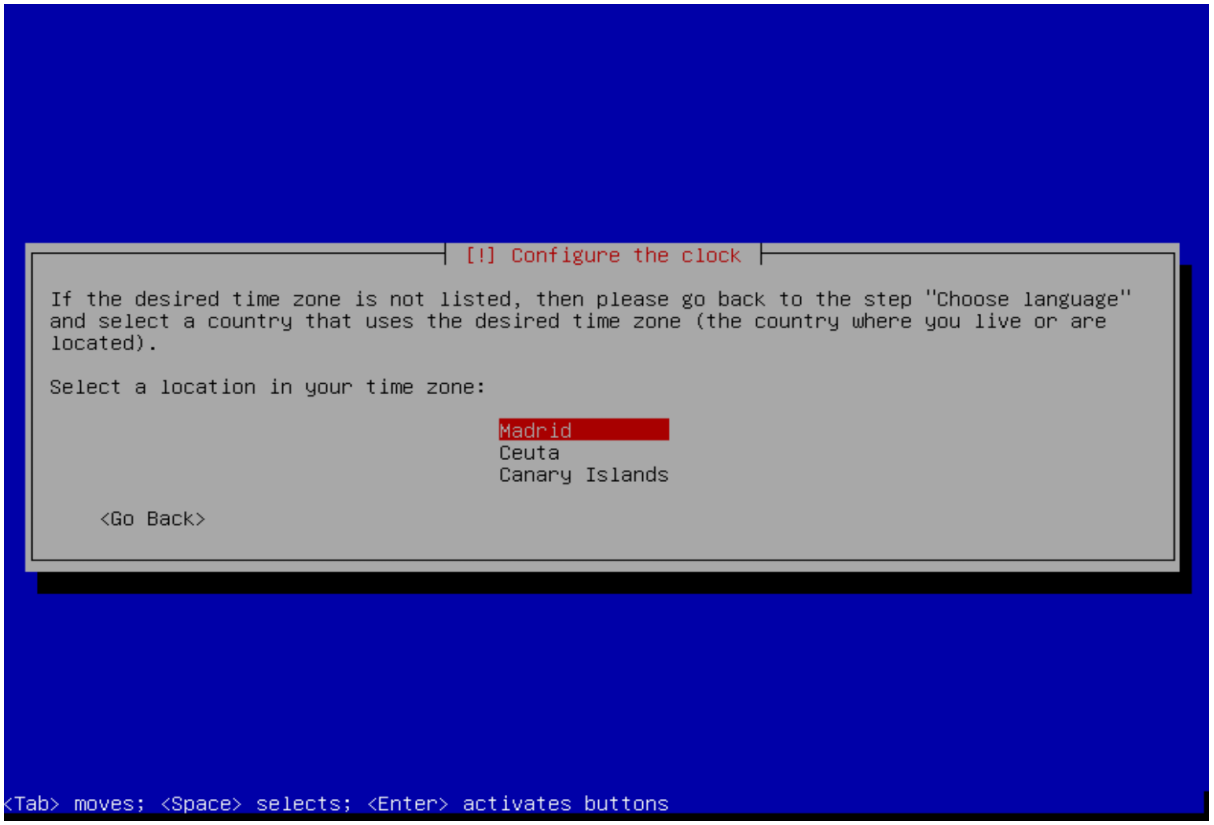
We don’t need a domain name so leave it empty.



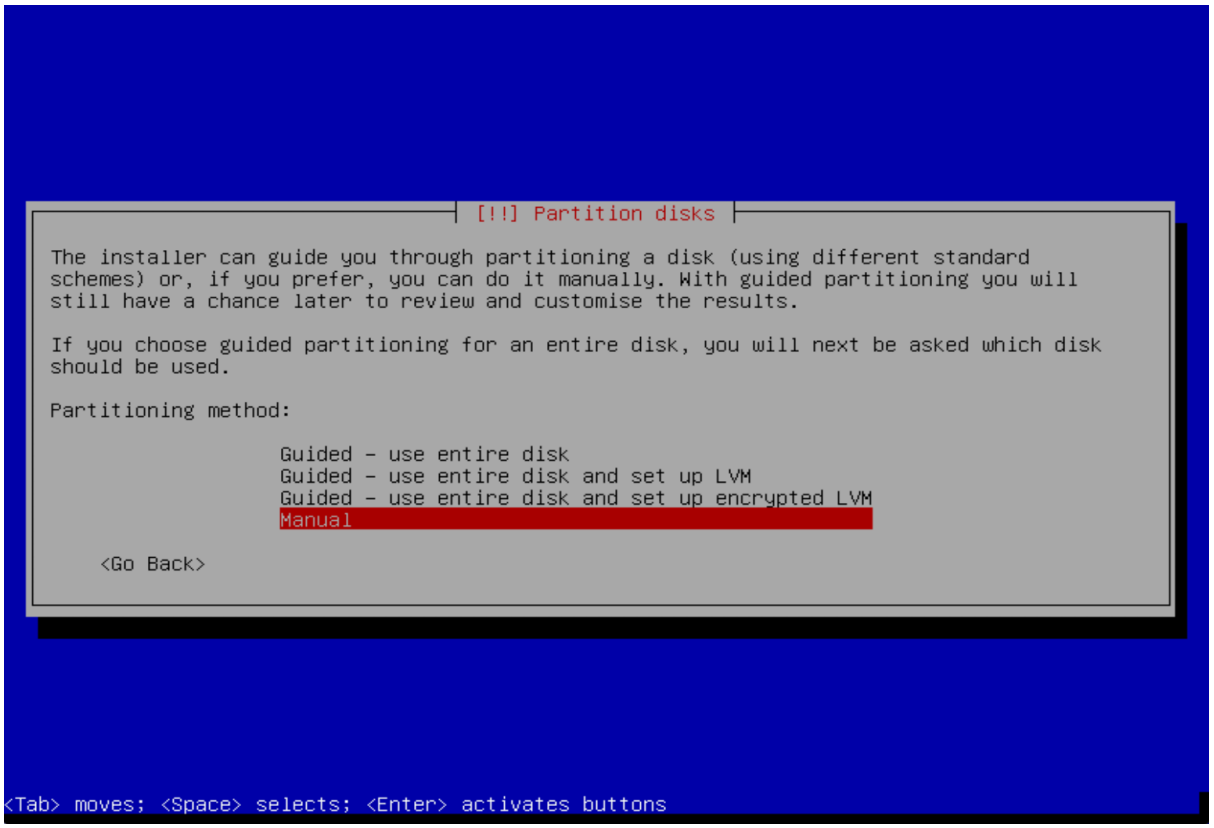
Now it ask us to set a root password. In my case I will use the same password for everything. “**Password42**”. Then, create the first standard user using our login.


[!!] Set up users and passwords
A user account will be created for you to use instead of the root account for non-administrative activities.
Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.
Full name for the new user:
Sergio Sanchez
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

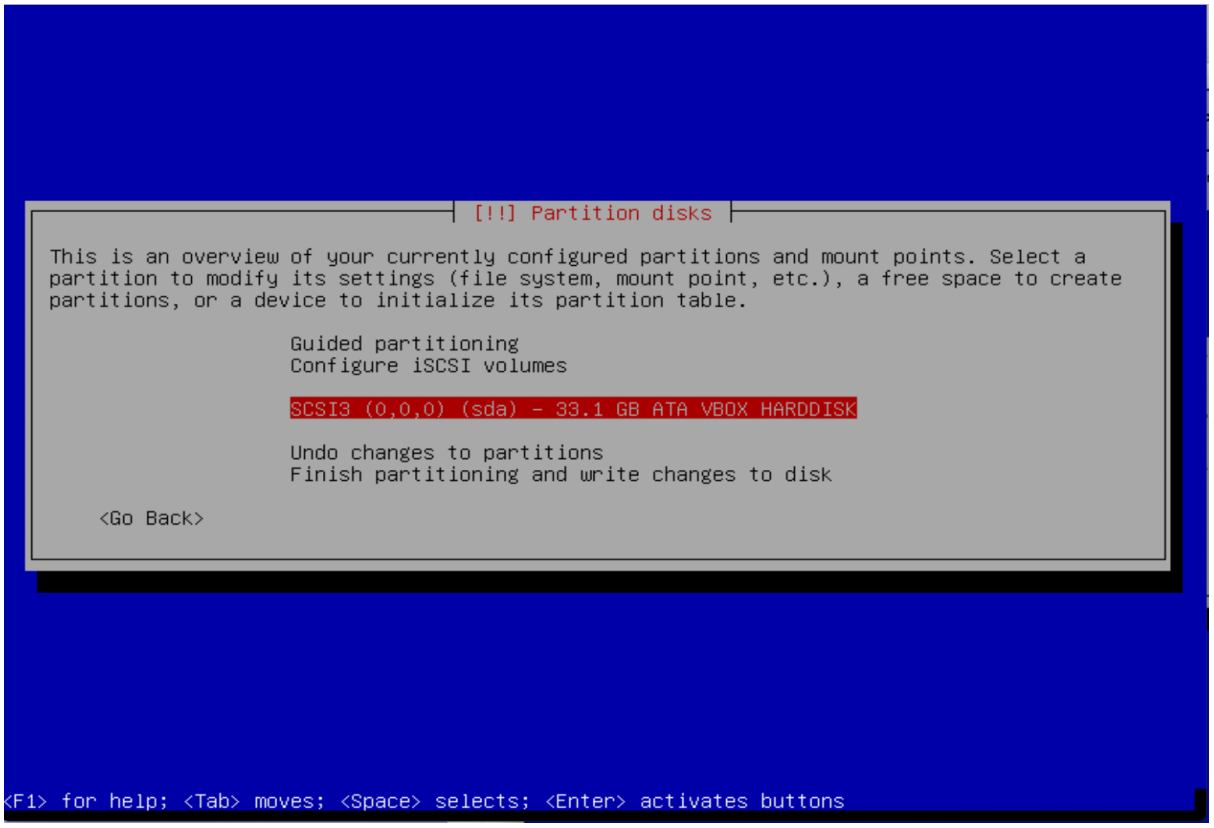

[!!] Set up users and passwords
Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.
Username for your account:
sersanch
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

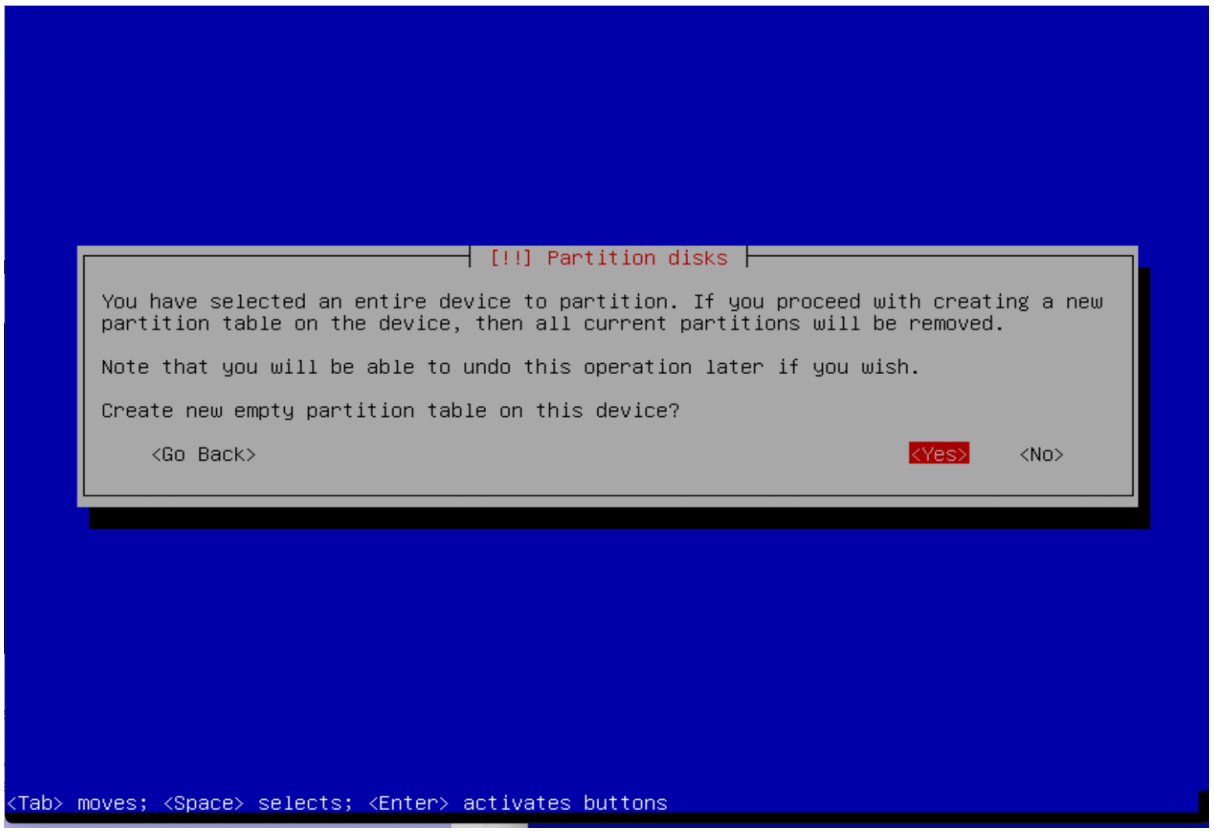


Now, the install program ask us if we want to make partitions. Select manual for customize the partitions as indicated in the subject.

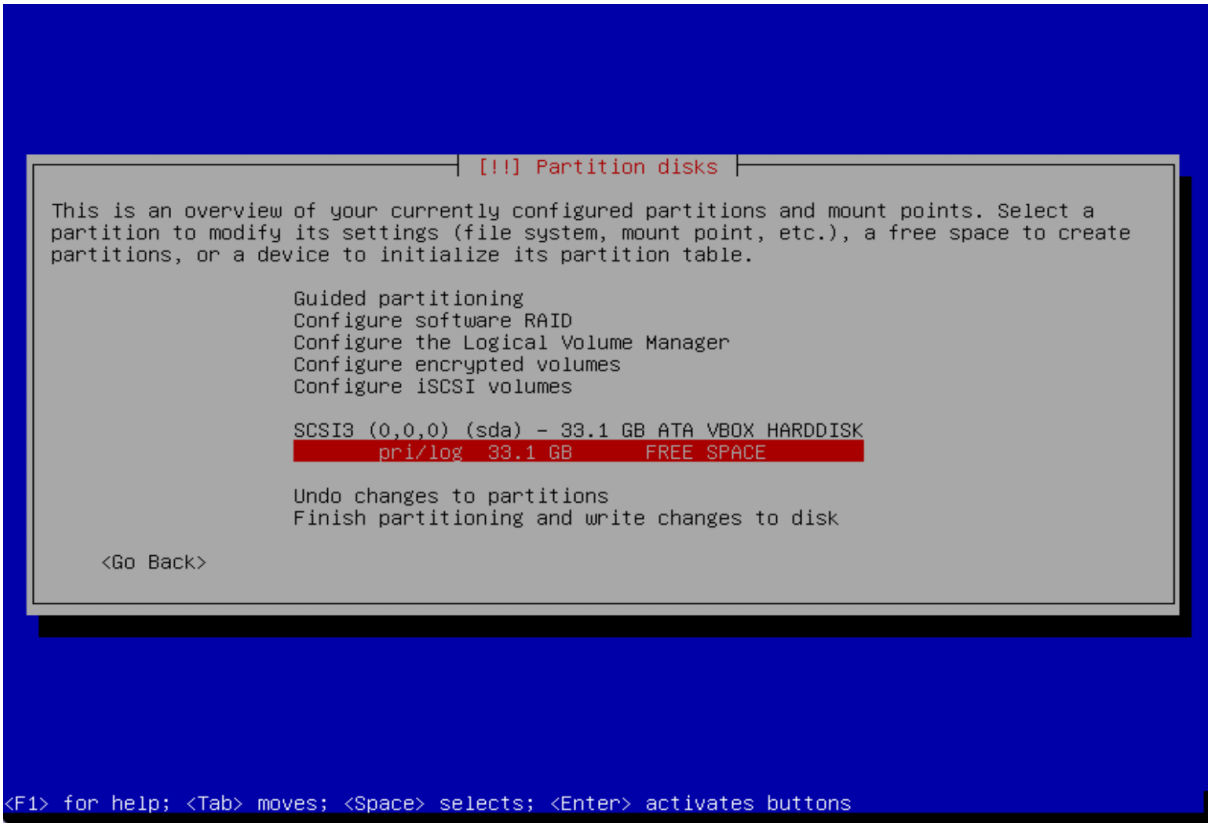


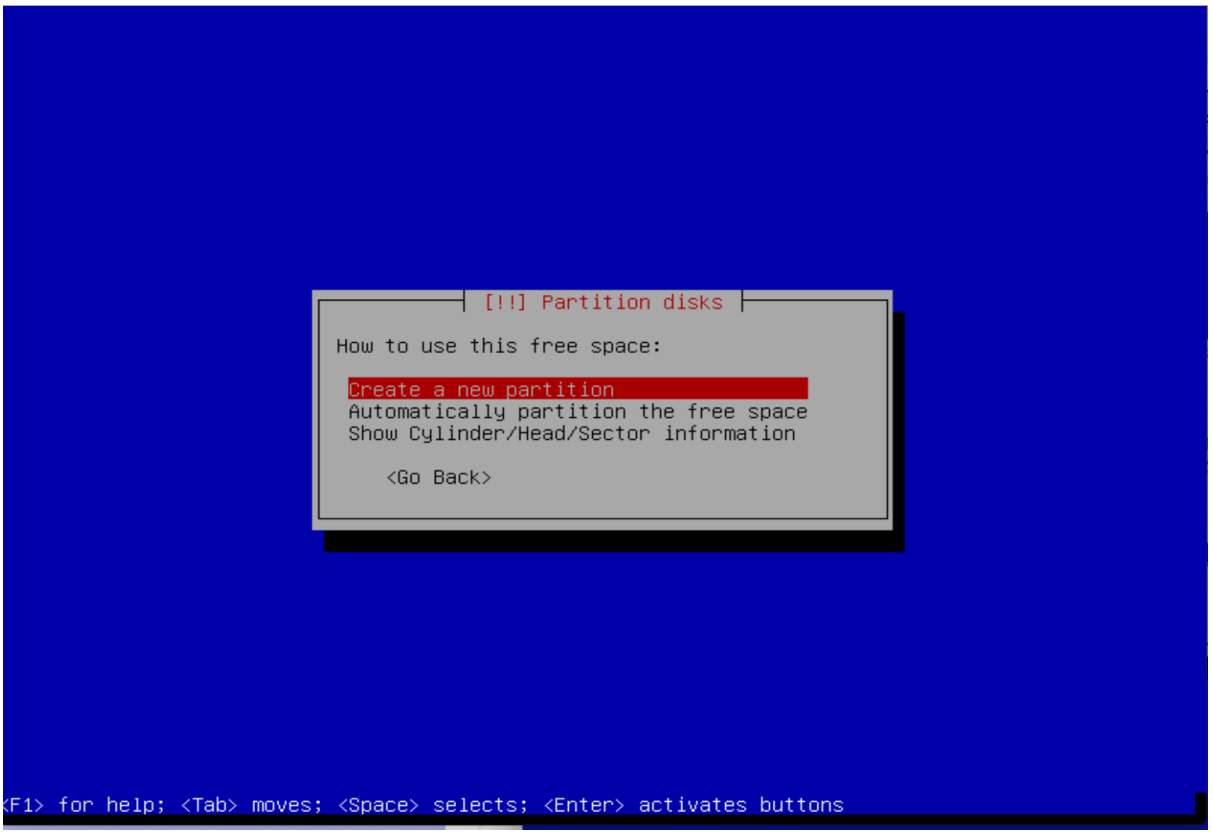
Select the main disk and create the first partition.



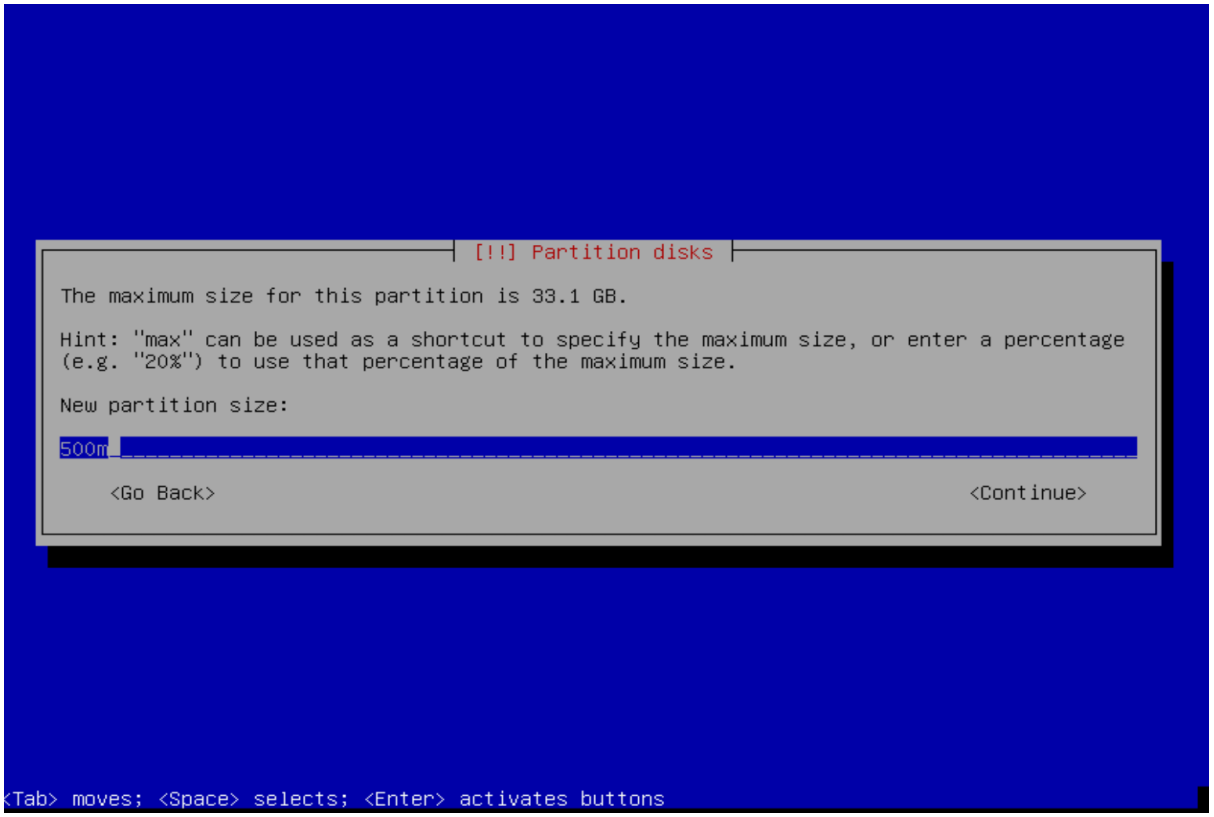


Let’s configure the created partition. Select it.

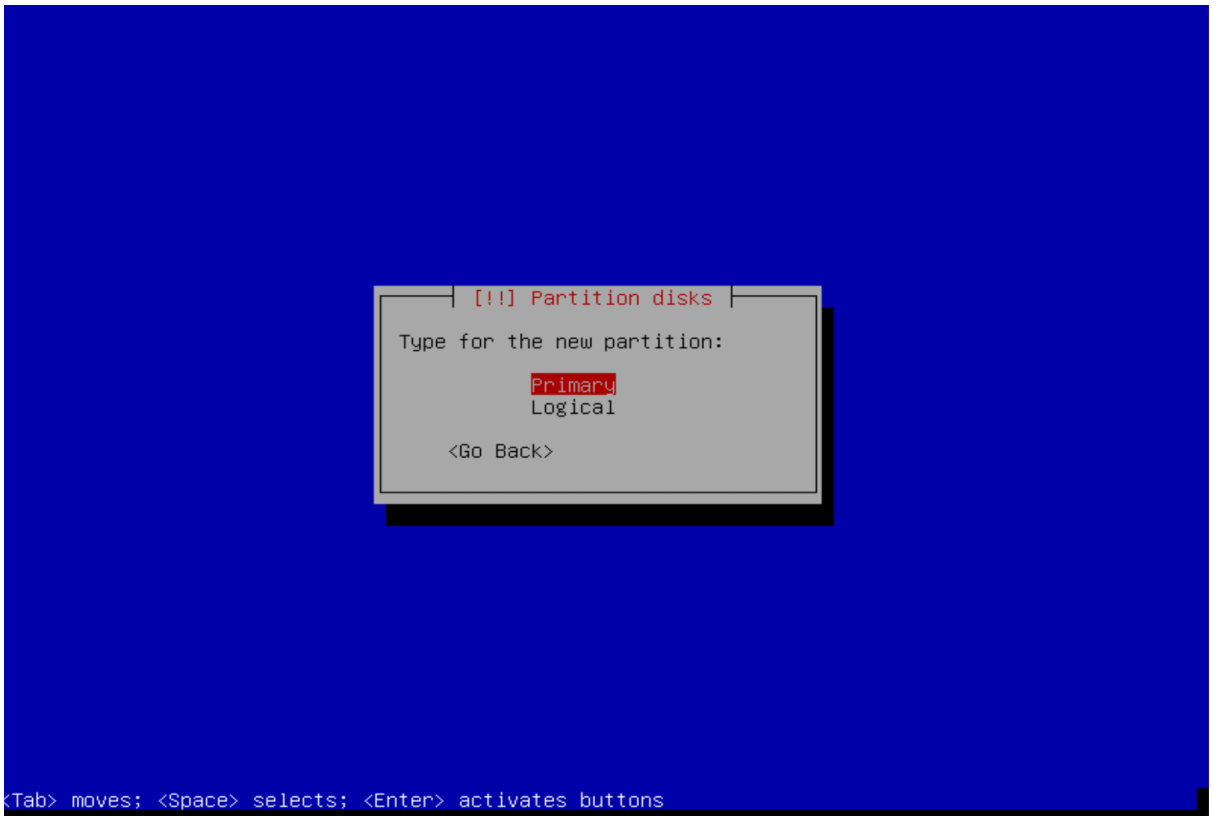




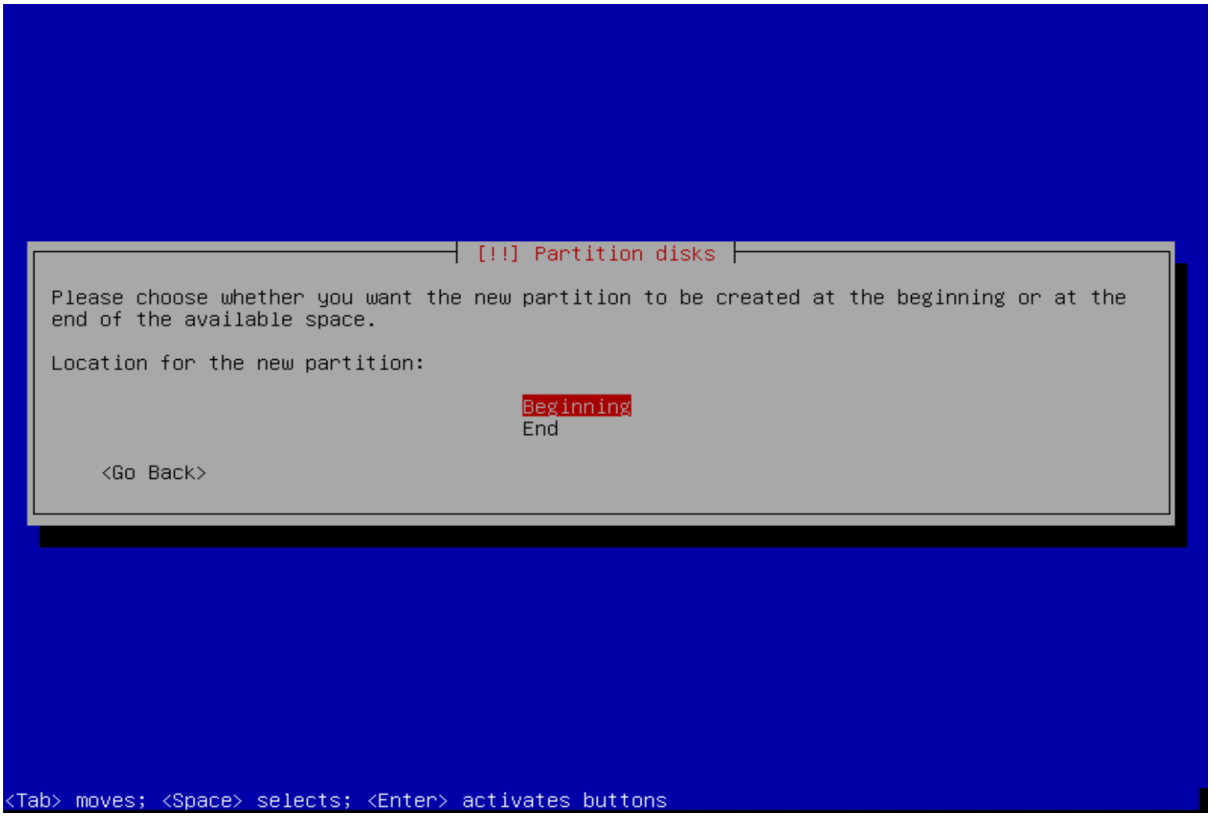
The space reserved is the same as indicated in the subject.



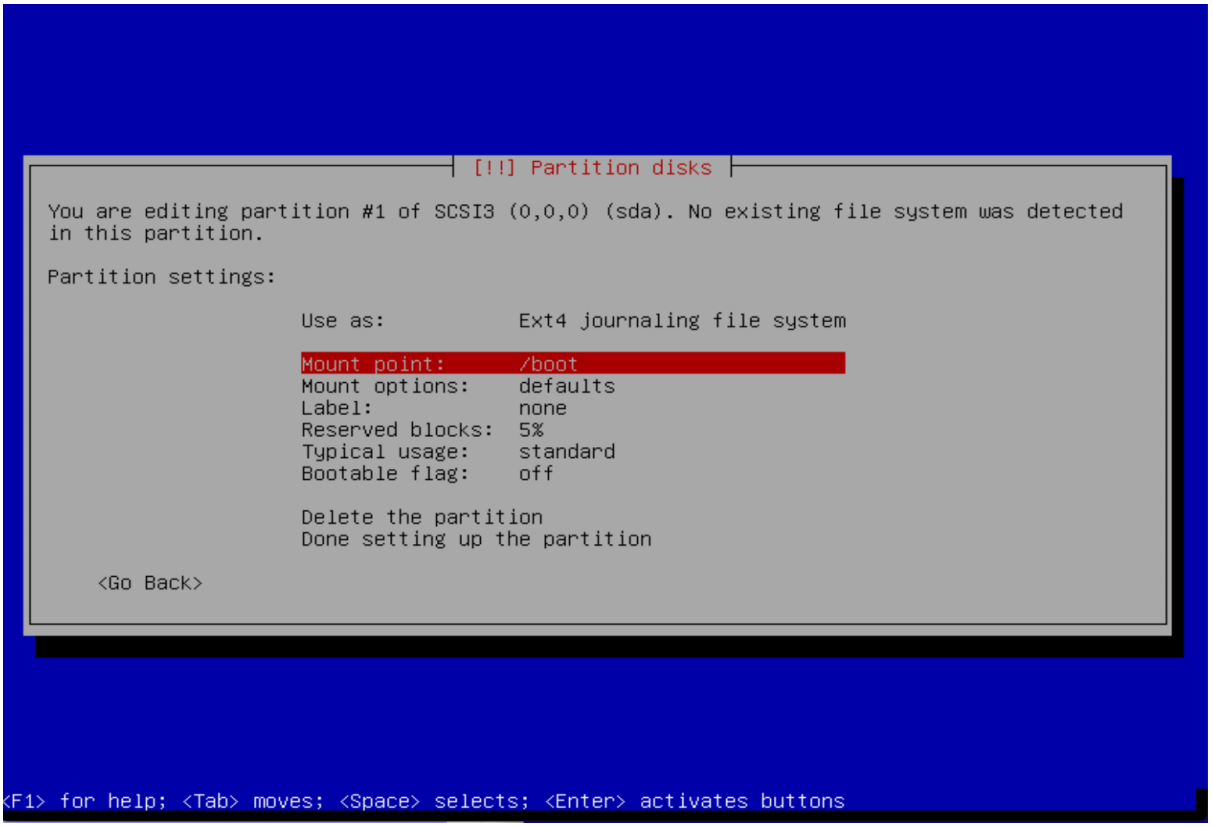
This partition will be primary. It will contain all the other logical partitions.

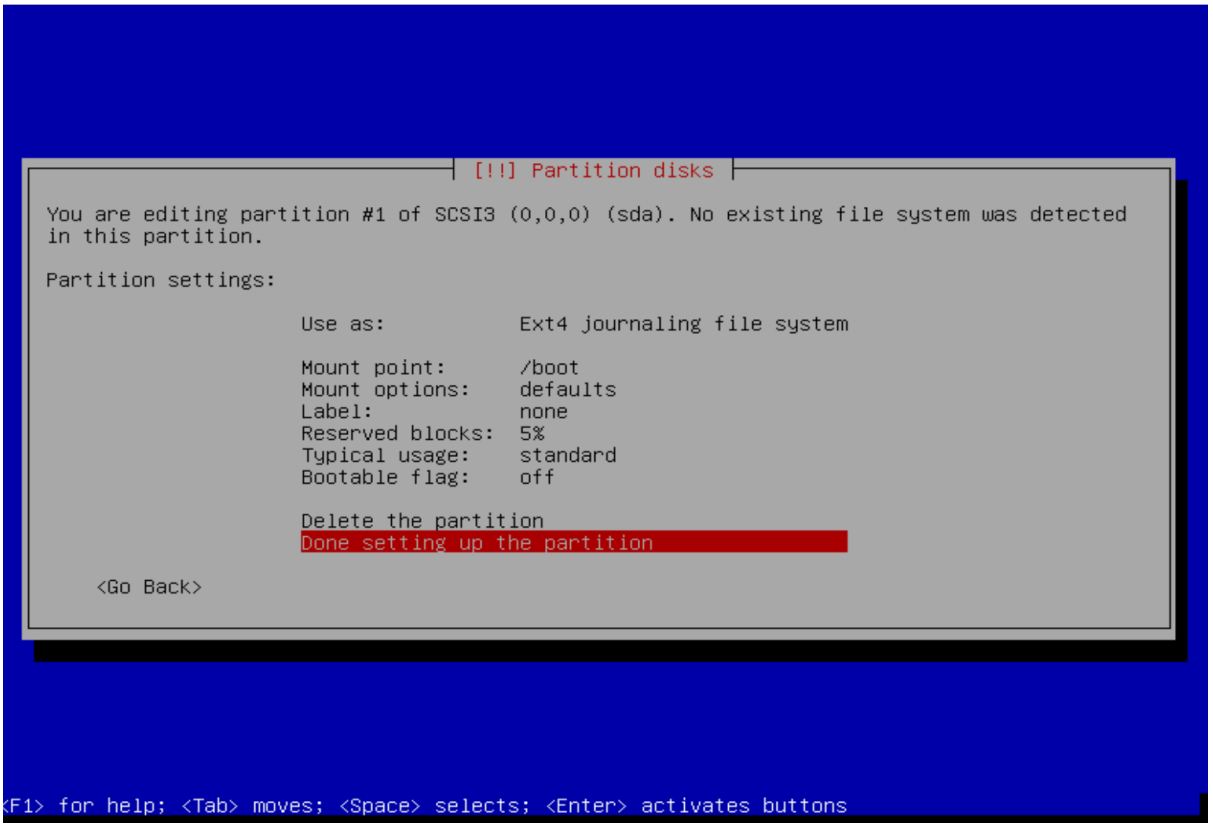


This partition will be located at the beginning of the memory.

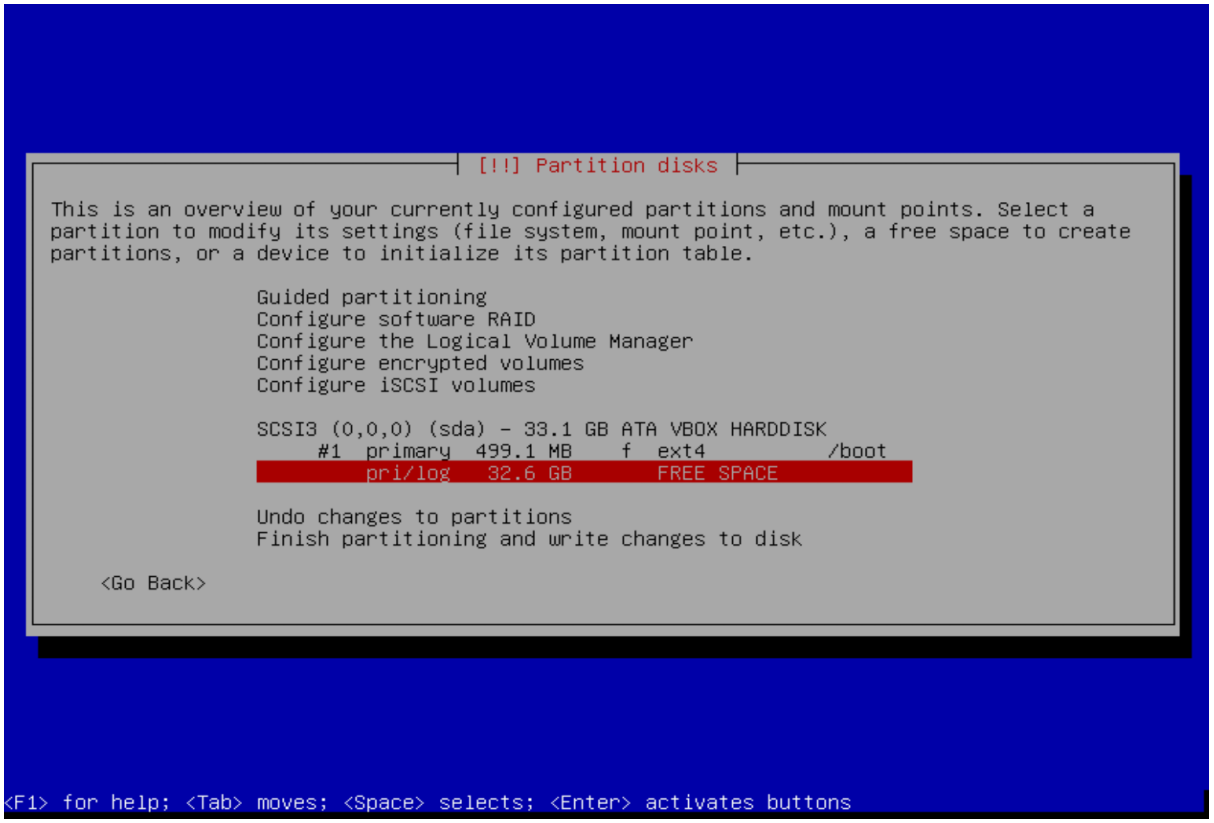


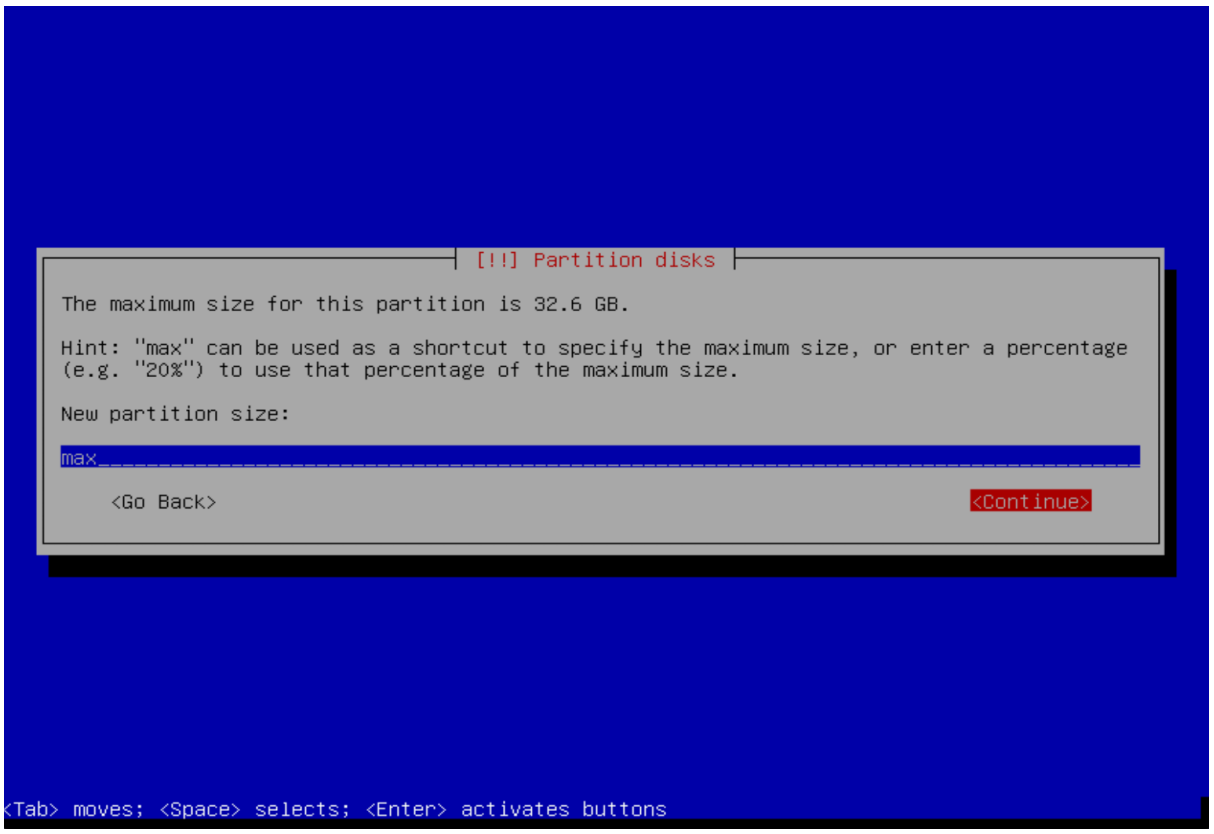
Configure the partition like the screenshot.
Ext4 → File system for Linux.
Mount point → /boot → Following the subject indications.

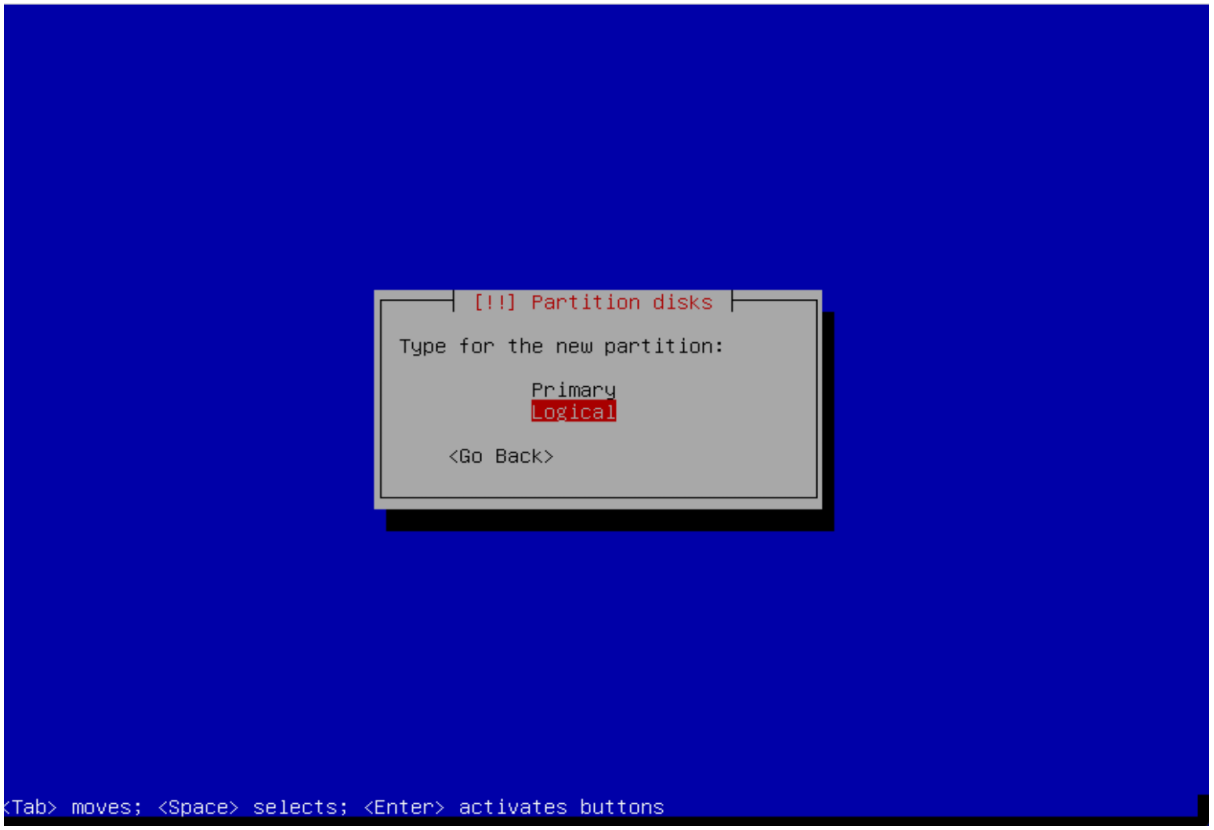


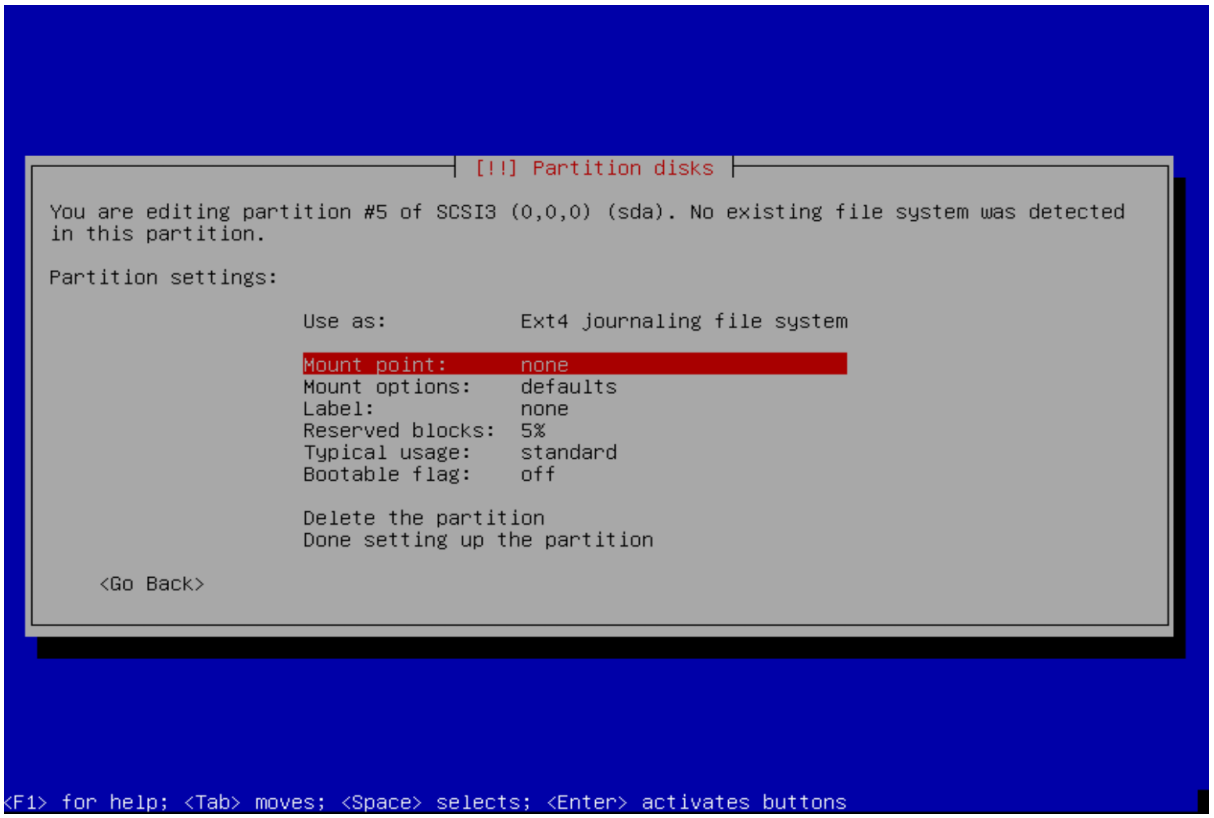


Next, let’s create the logical partition with the rest of the space available.

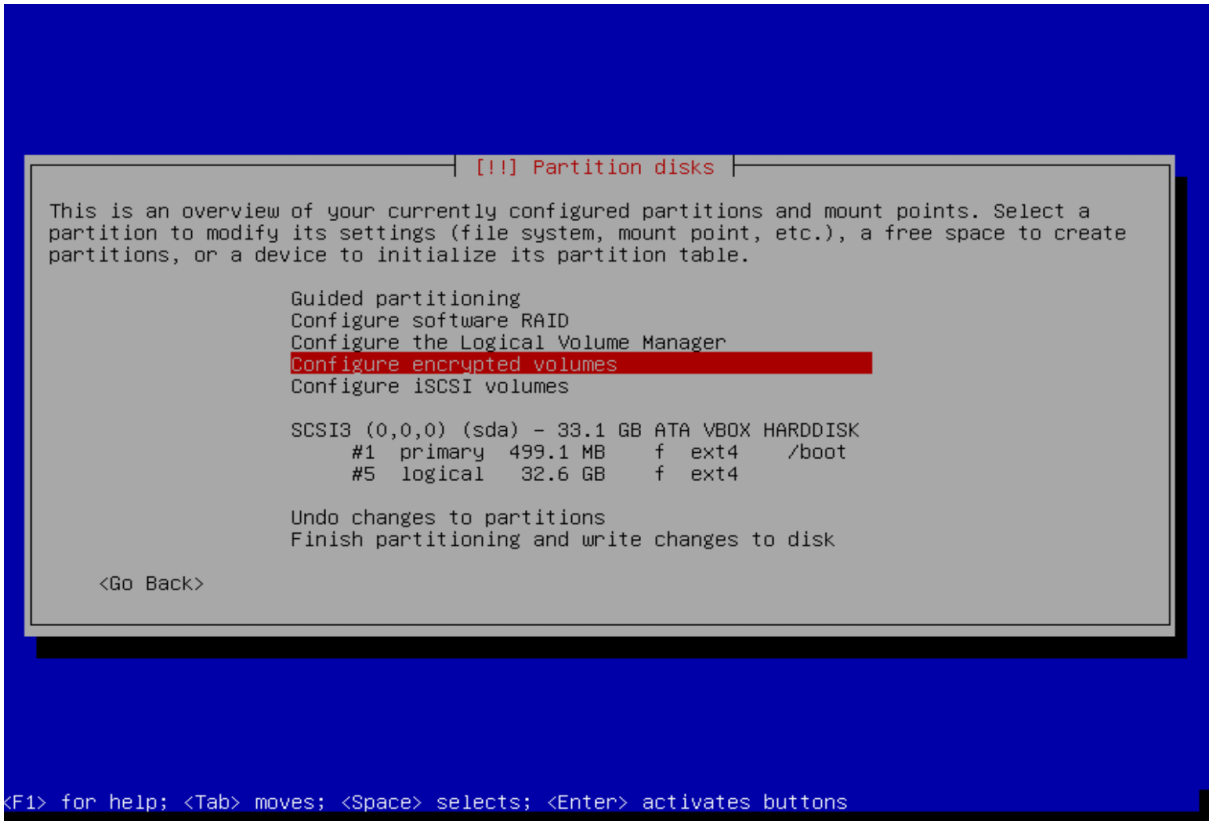

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI3 (0,0,0) (sda) - 33.1 GB ATA VBOX HARDDISK
#1 primary 499.1 MB f ext4 /boot
pri/log 32.6 GB FREE SPACE
Undo changes to partitions
Finish partitioning and write changes to disk
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

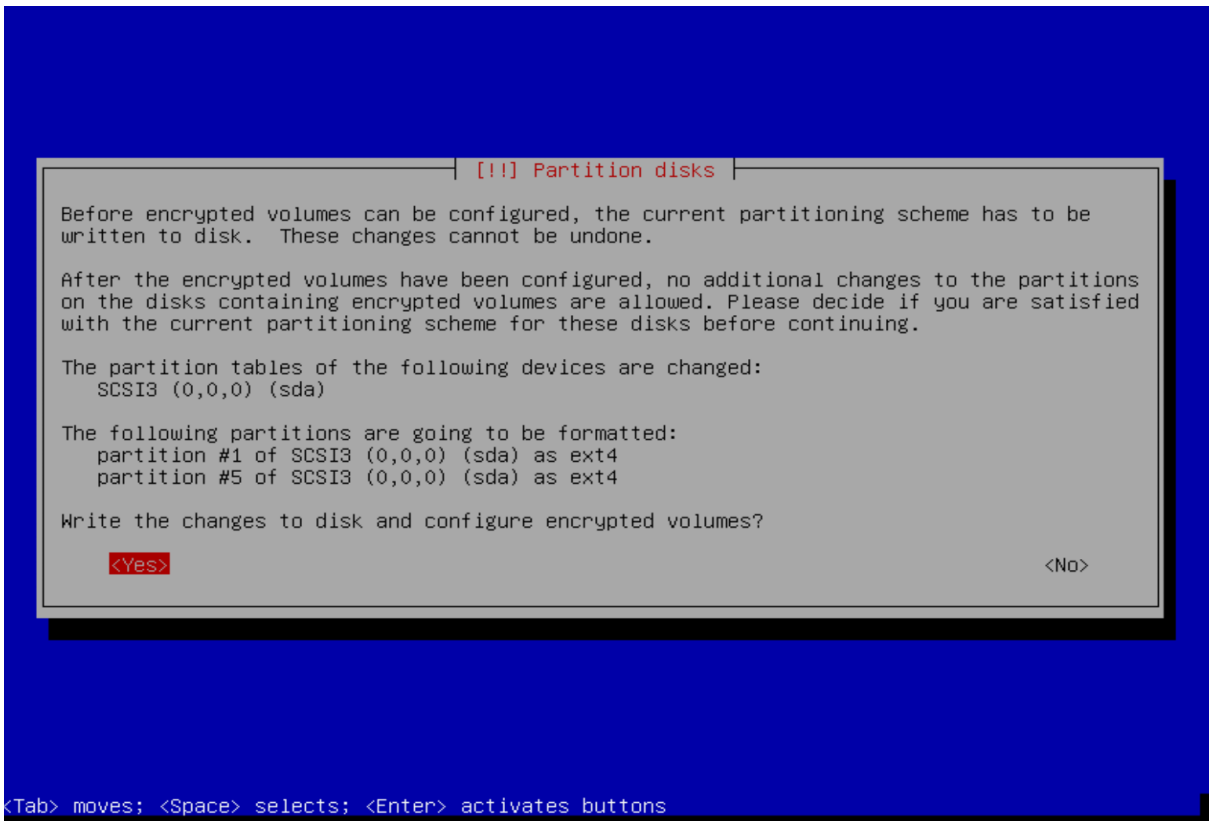

[!!] Partition disks
The maximum size for this partition is 32.6 GB.
Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage (e.g. "20%") to use that percentage of the maximum size.
New partition size:
max
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

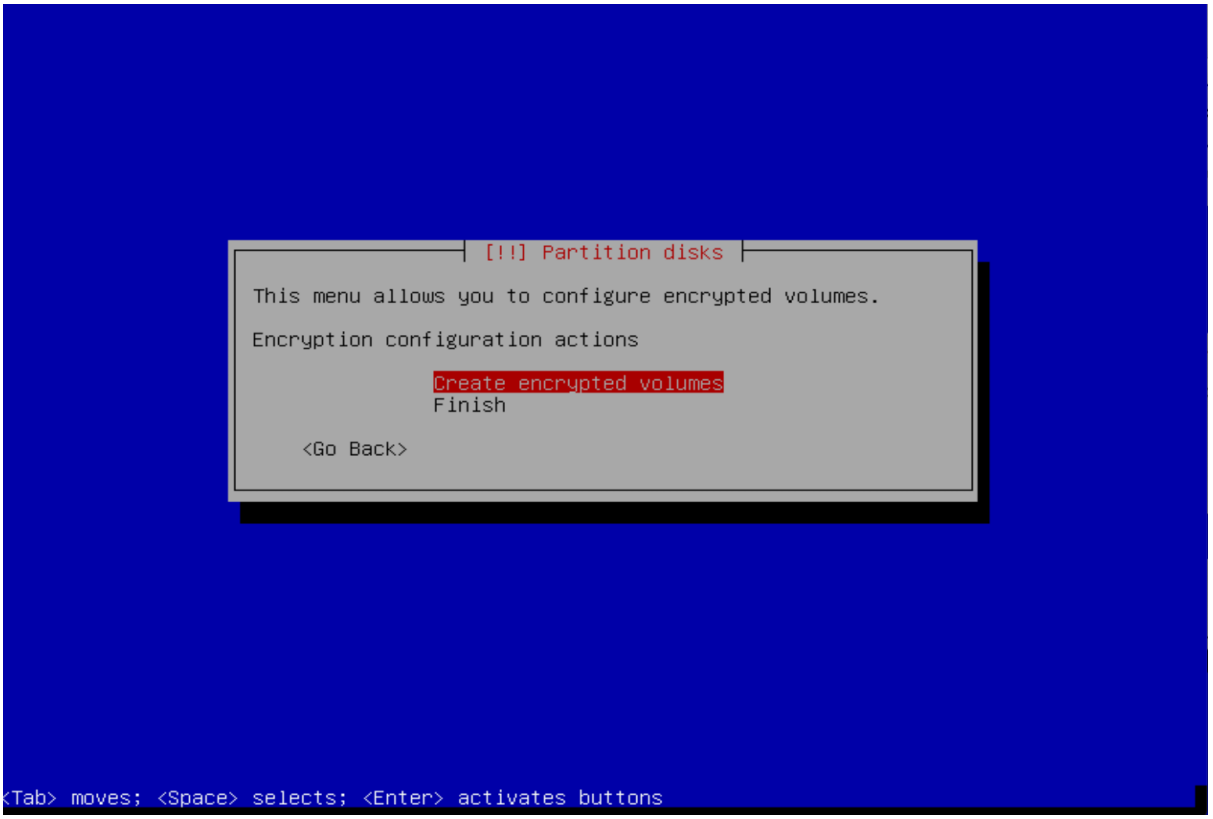




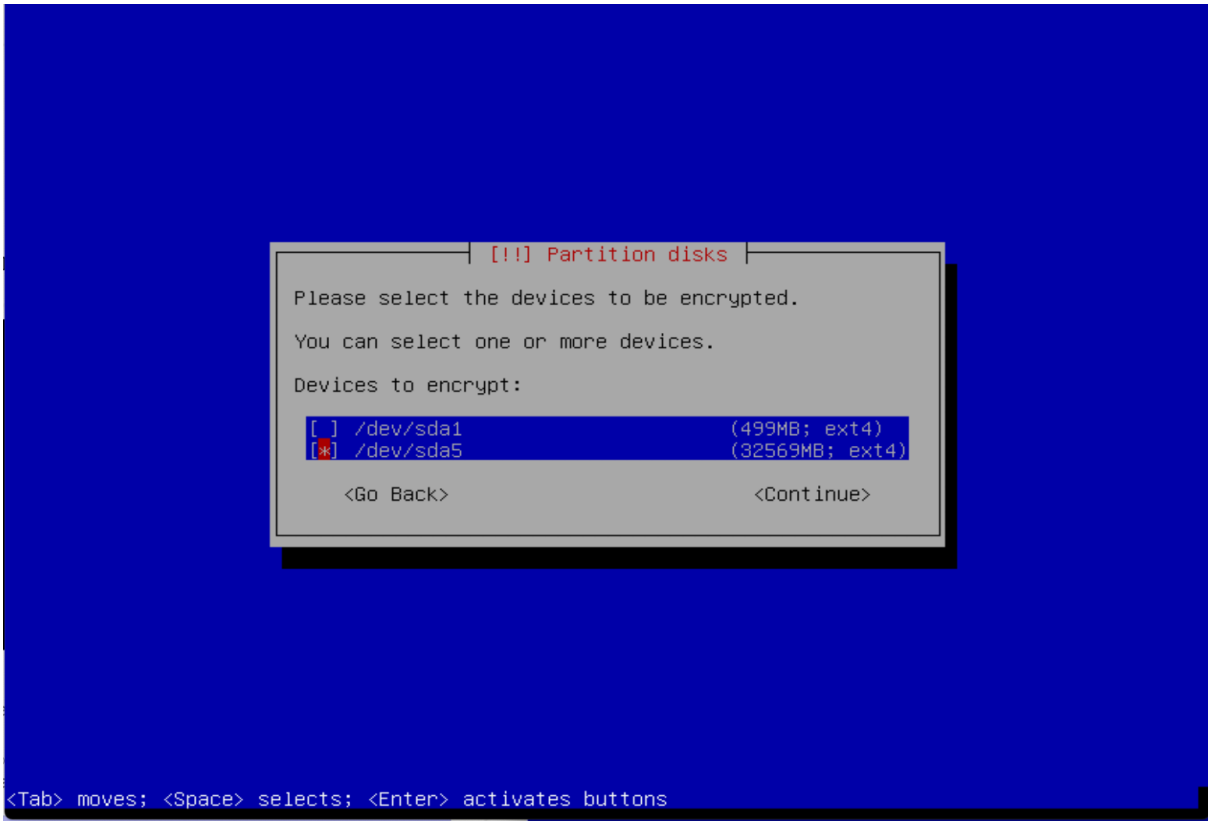
Now, let’s configure the encryption of the partitions.

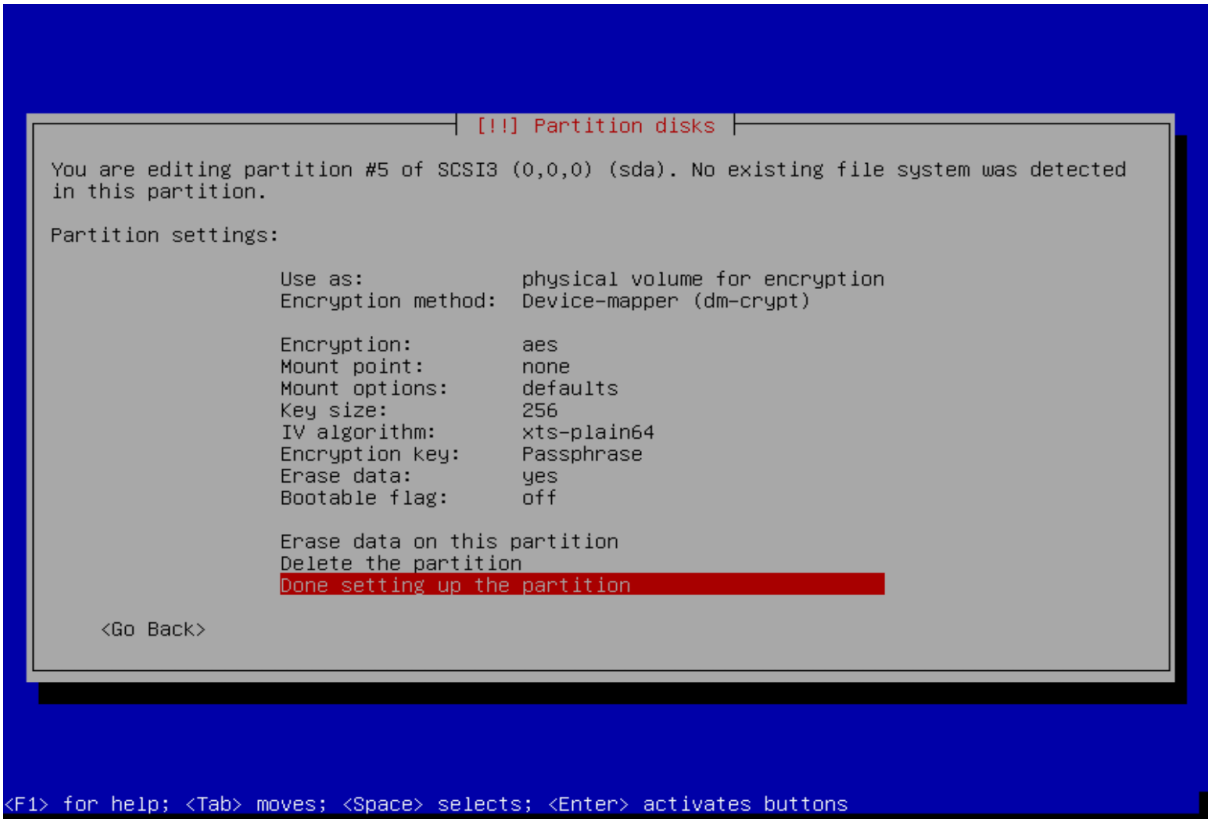

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI3 (0,0,0) (sda) - 33.1 GB ATA VBOX HARDDISK
#1 primary 499.1 MB f ext4 /boot
#5 logical 32.6 GB f ext4
Undo changes to partitions
Finish partitioning and write changes to disk
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

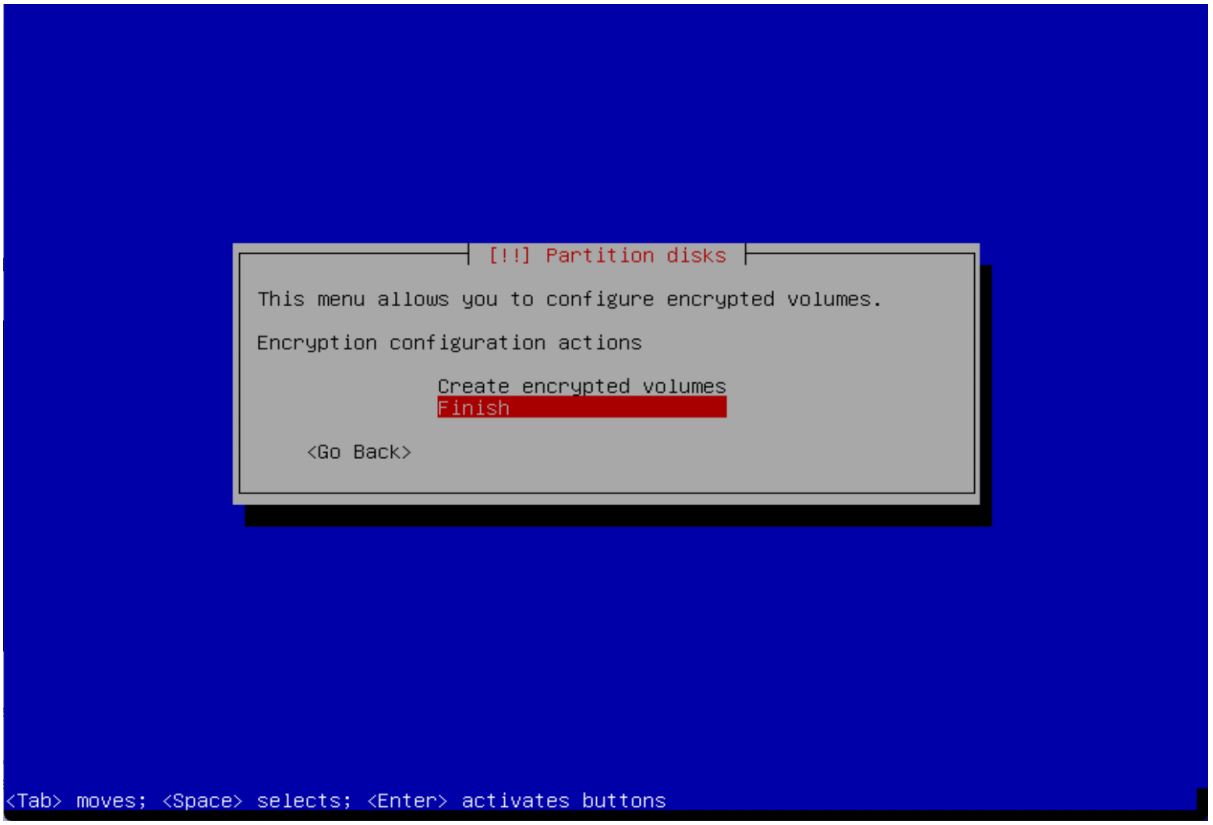

[!!] Partition disks
Before encrypted volumes can be configured, the current partitioning scheme has to be written to disk. These changes cannot be undone.
After the encrypted volumes have been configured, no additional changes to the partitions on the disks containing encrypted volumes are allowed. Please decide if you are satisfied with the current partitioning scheme for these disks before continuing.
The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as ext4
Write the changes to disk and configure encrypted volumes?
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons

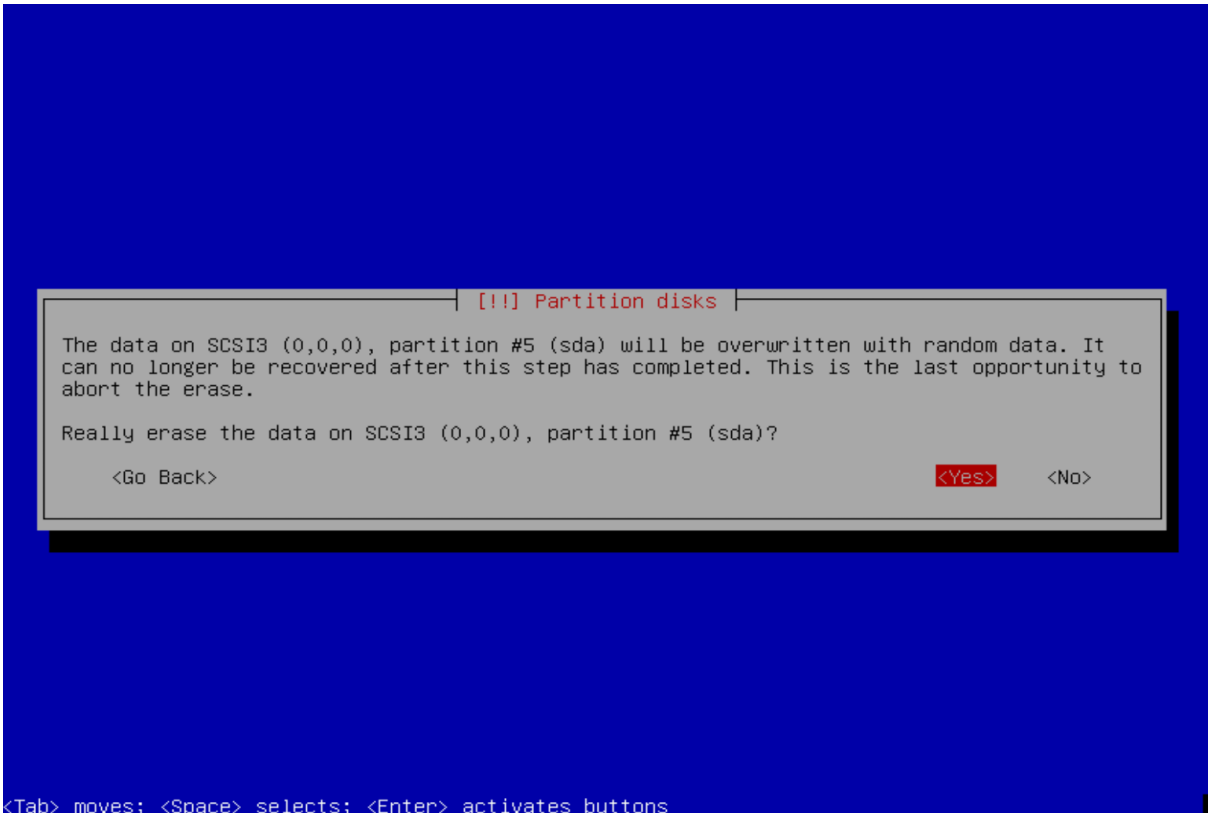


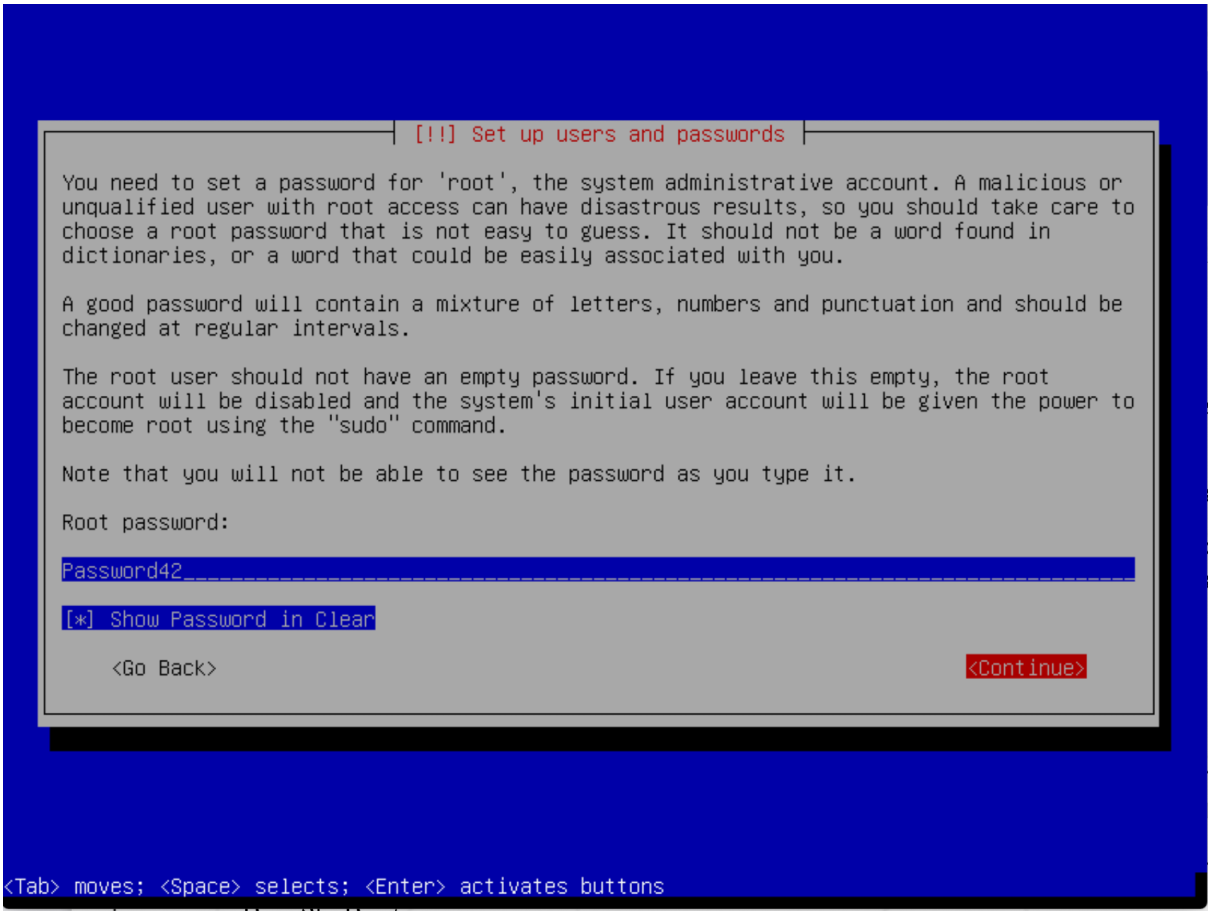
Select the sda5, the logical partition. The password will be the same as the root and users.

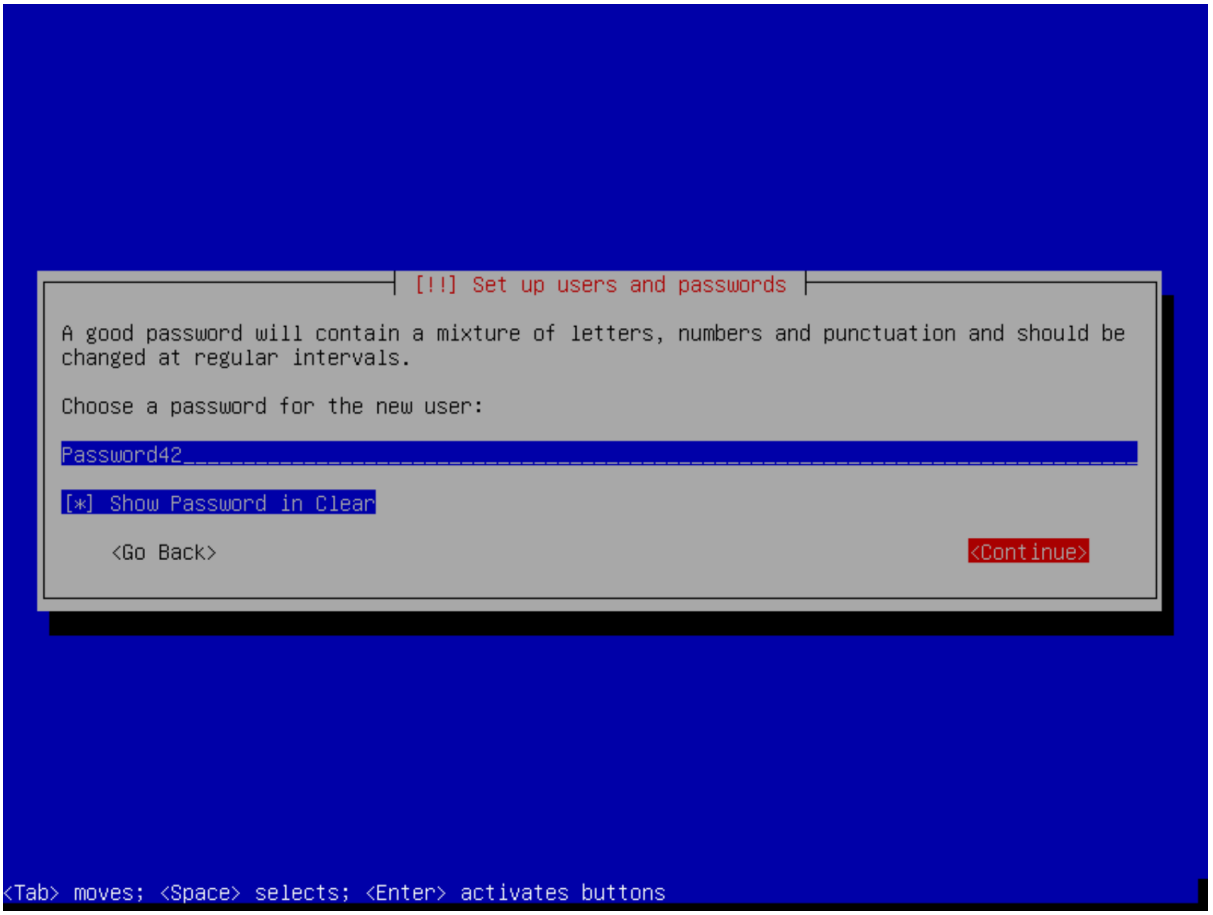

[!!] Partition disks
Please select the devices to be encrypted.
You can select one or more devices.
Devices to encrypt:
[ ] /dev/sda1 (499MB; ext4)
[*] /dev/sda5 (32569MB; ext4)
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Partition disks
You are editing partition #5 of SCSI3 (0,0,0) (sda). No existing file system was detected in this partition.
Partition settings:
Use as: physical volume for encryption
Encryption method: Device-mapper (dm-crypt)
Encryption: aes
Mount point: none
Mount options: defaults
Key size: 256
IV algorithm: xts-plain64
Encryption key: Passphrase
Erase data: yes
Bootable flag: off
Erase data on this partition
Delete the partition
Done setting up the partition
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

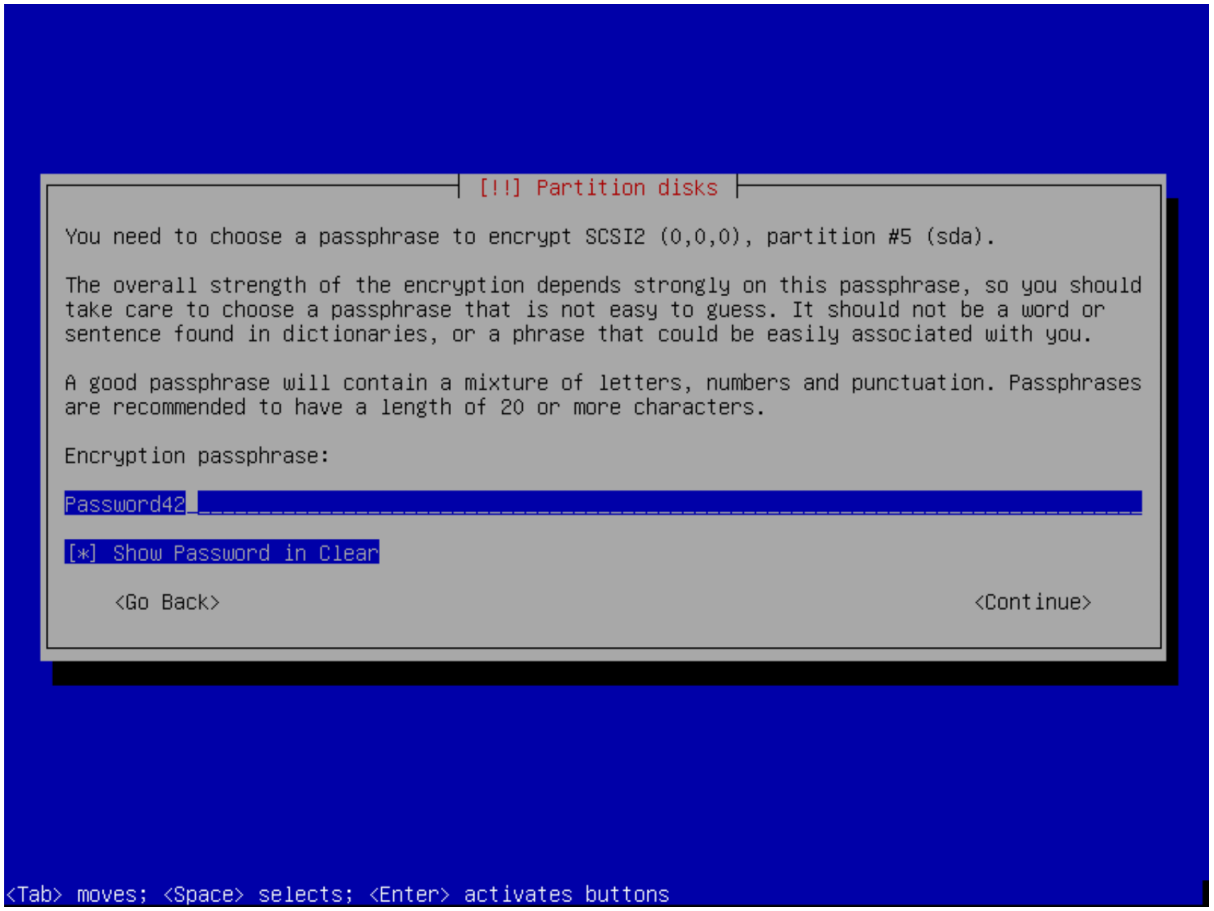

[!!] Partition disks
This menu allows you to configure encrypted volumes.
Encryption configuration actions
Create encrypted volumes
Finish
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

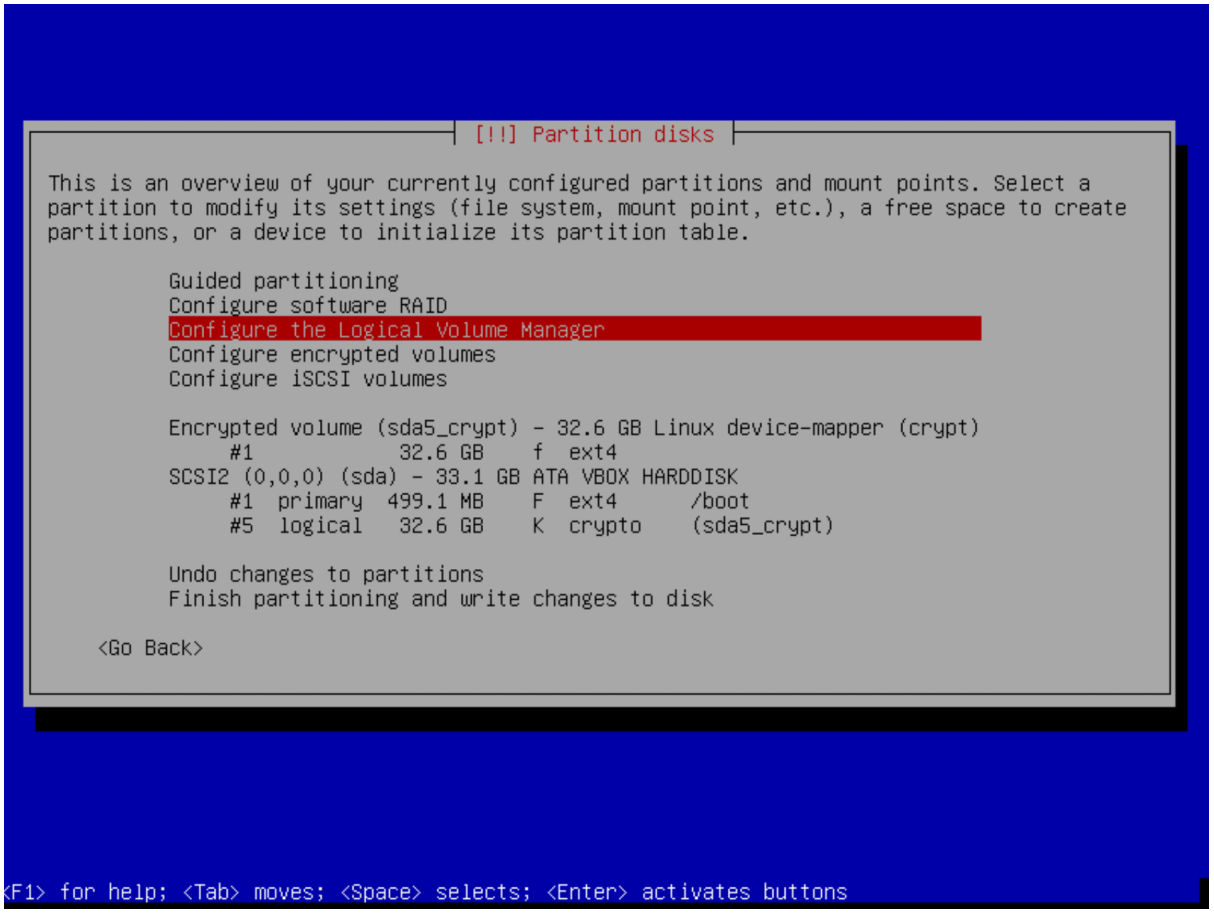

[!!] Partition disks
The data on SCSI3 (0,0,0), partition #5 (sda) will be overwritten with random data. It can no longer be recovered after this step has completed. This is the last opportunity to abort the erase.
Really erase the data on SCSI3 (0,0,0), partition #5 (sda)?
<Go Back>
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons



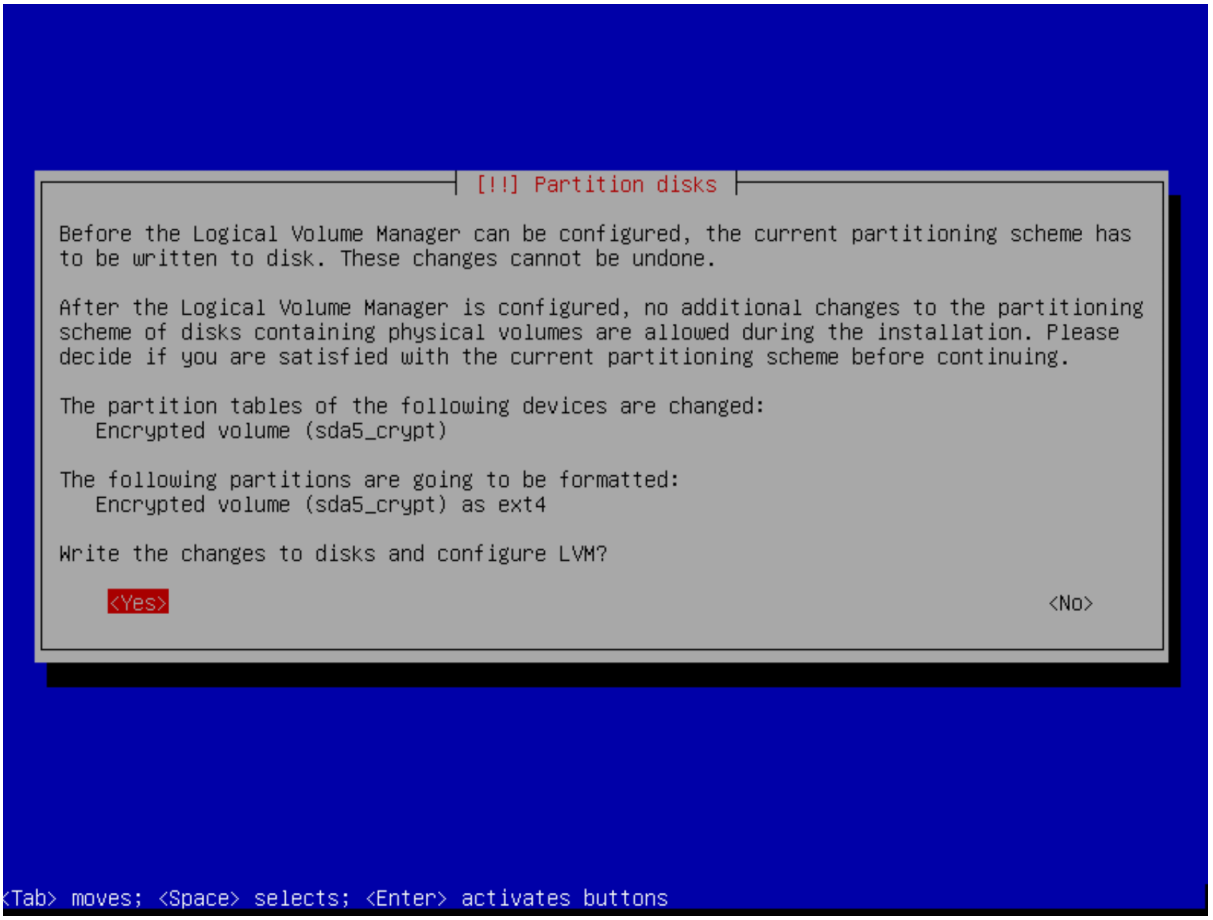


sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus

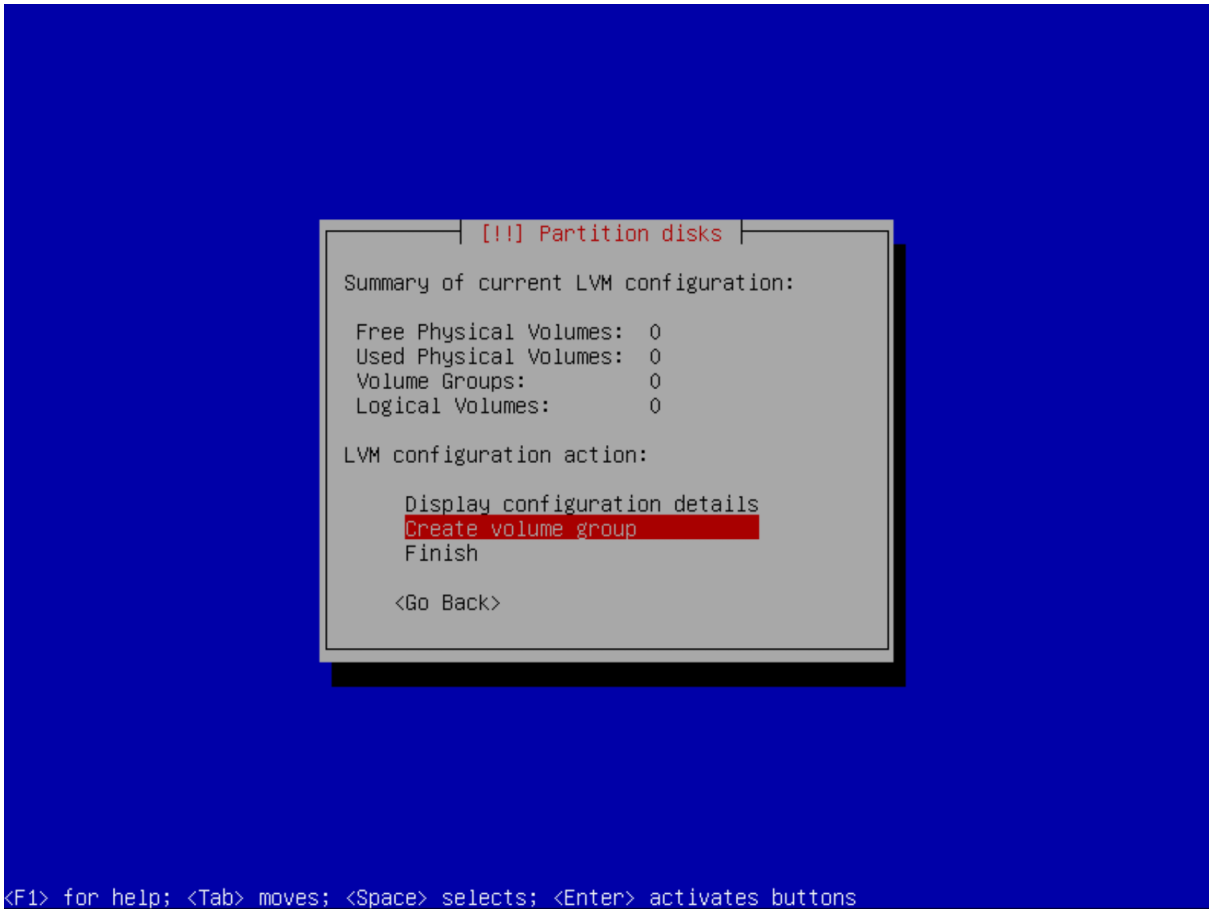

[!!] Partition disks
You need to choose a passphrase to encrypt SCSI2 (0,0,0), partition #5 (sda).
The overall strength of the encryption depends strongly on this passphrase, so you should take care to choose a passphrase that is not easy to guess. It should not be a word or sentence found in dictionaries, or a phrase that could be easily associated with you.
A good passphrase will contain a mixture of letters, numbers and punctuation. Passphrases are recommended to have a length of 20 or more characters.
Encryption passphrase:
Password42
[*] Show Password in Clear
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

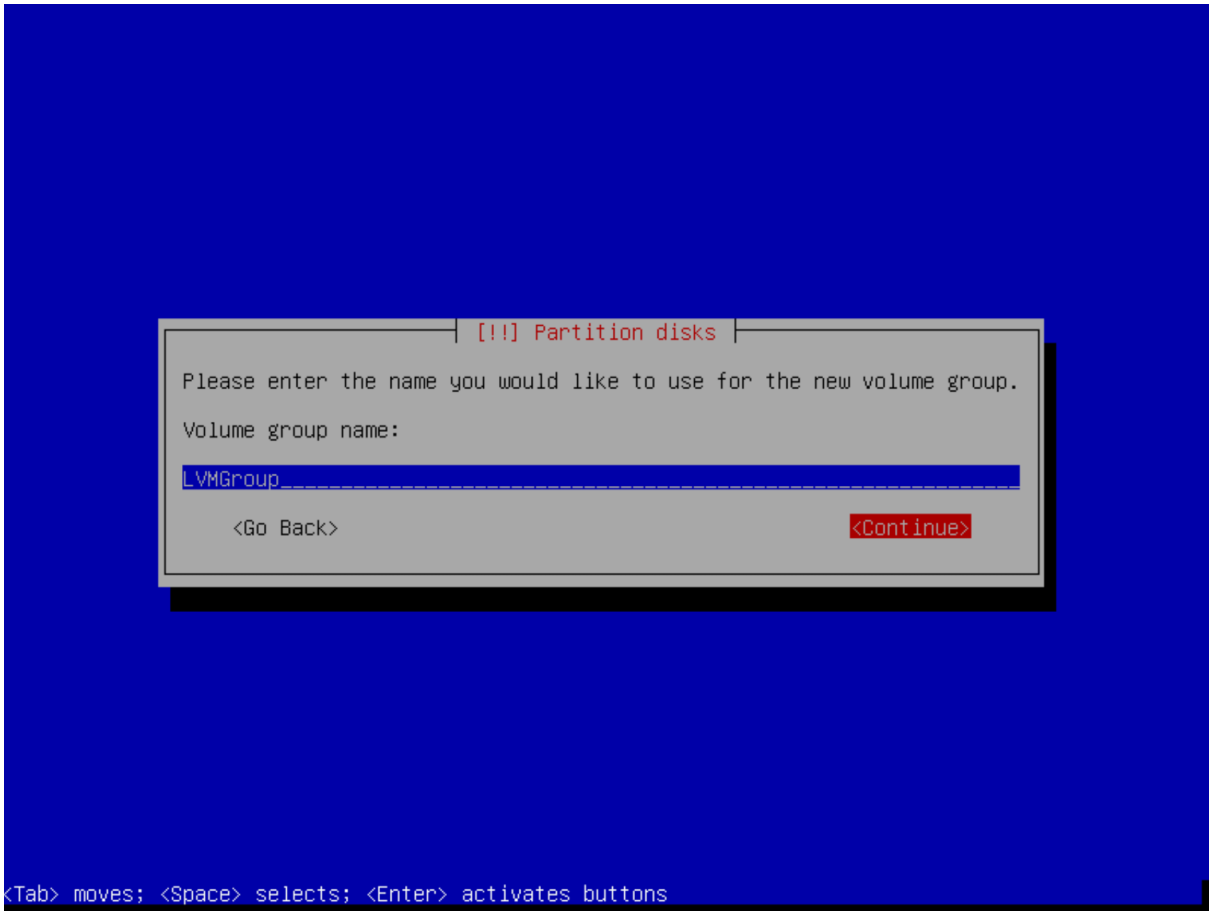

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
Encrypted volume (sda5_crypt) - 32.6 GB Linux device-mapper (crypt)
#1 32.6 GB f ext4
SCSI2 (0,0,0) (sda) - 33.1 GB ATA VBOX HARDDISK
#1 primary 499.1 MB F ext4 /boot
#5 logical 32.6 GB K crypto (sda5_crypt)
Undo changes to partitions
Finish partitioning and write changes to disk
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

Now that the encrypted volumes are created, let’s configure it.

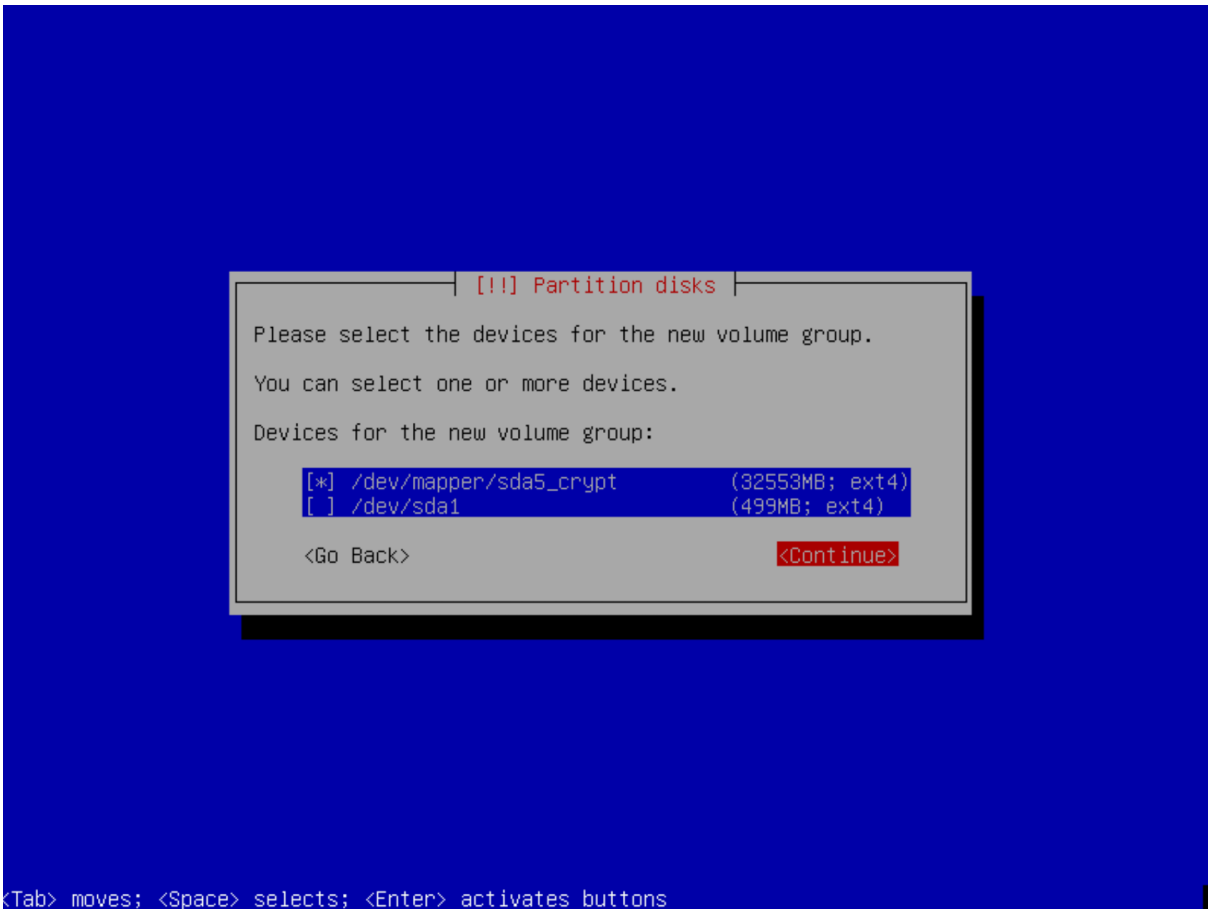


First, create a volume group for LVM (Logical Volume Manager). The name is the same as shown in the subject.

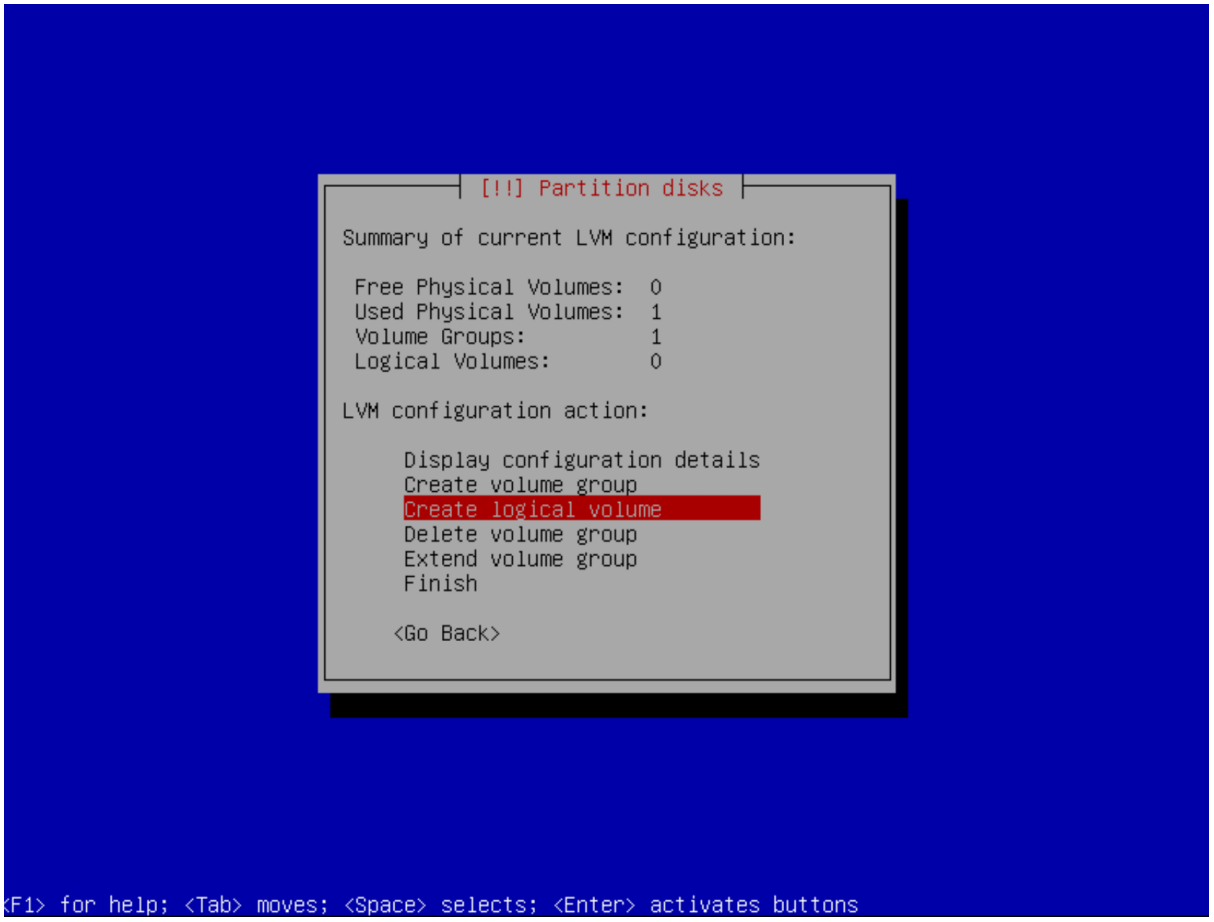

[!!] Partition disks
Summary of current LVM configuration:
Free Physical Volumes: 0
Used Physical Volumes: 0
Volume Groups: 0
Logical Volumes: 0
LVM configuration action:
Display configuration details
Create volume group
Finish
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

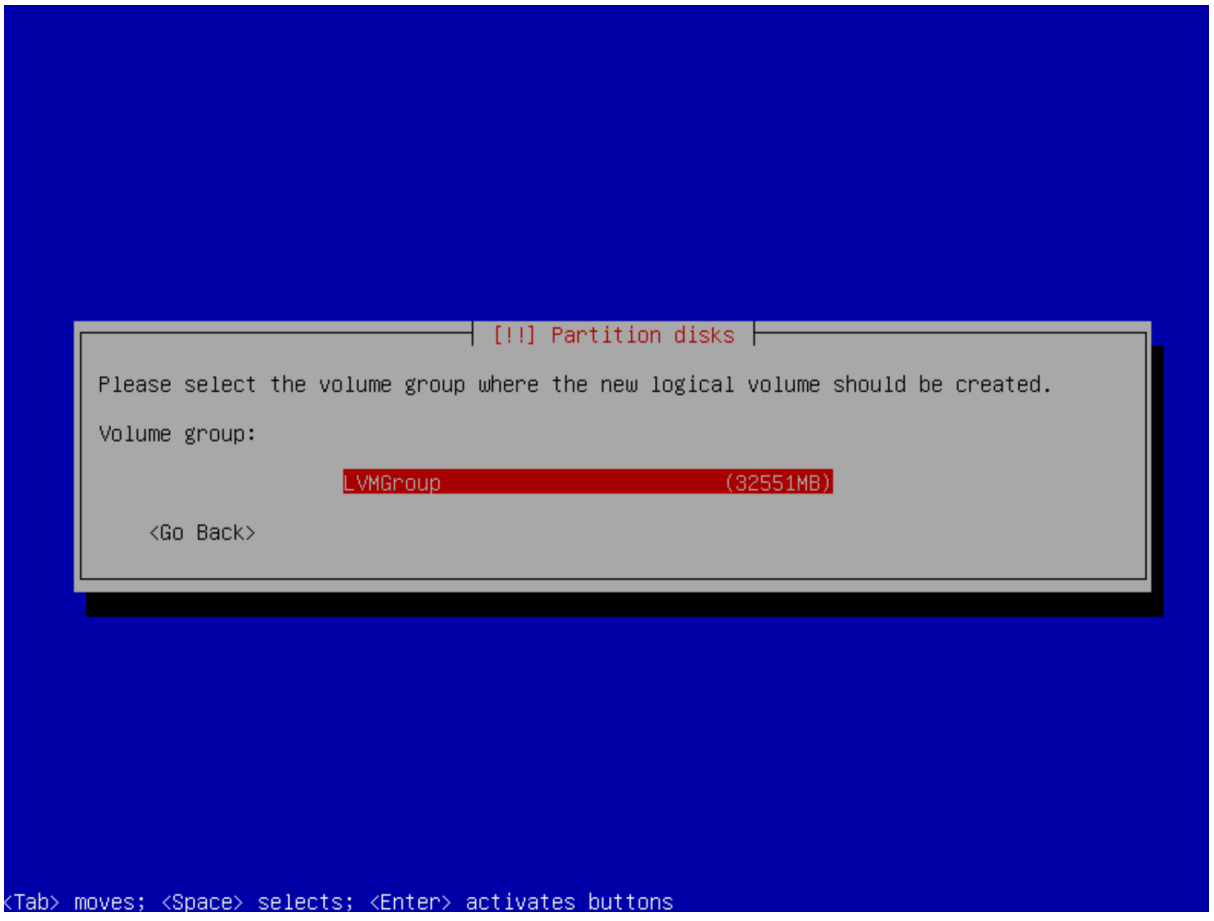

[!!] Partition disks
Please enter the name you would like to use for the new volume group.
Volume group name:
LVMGroup
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

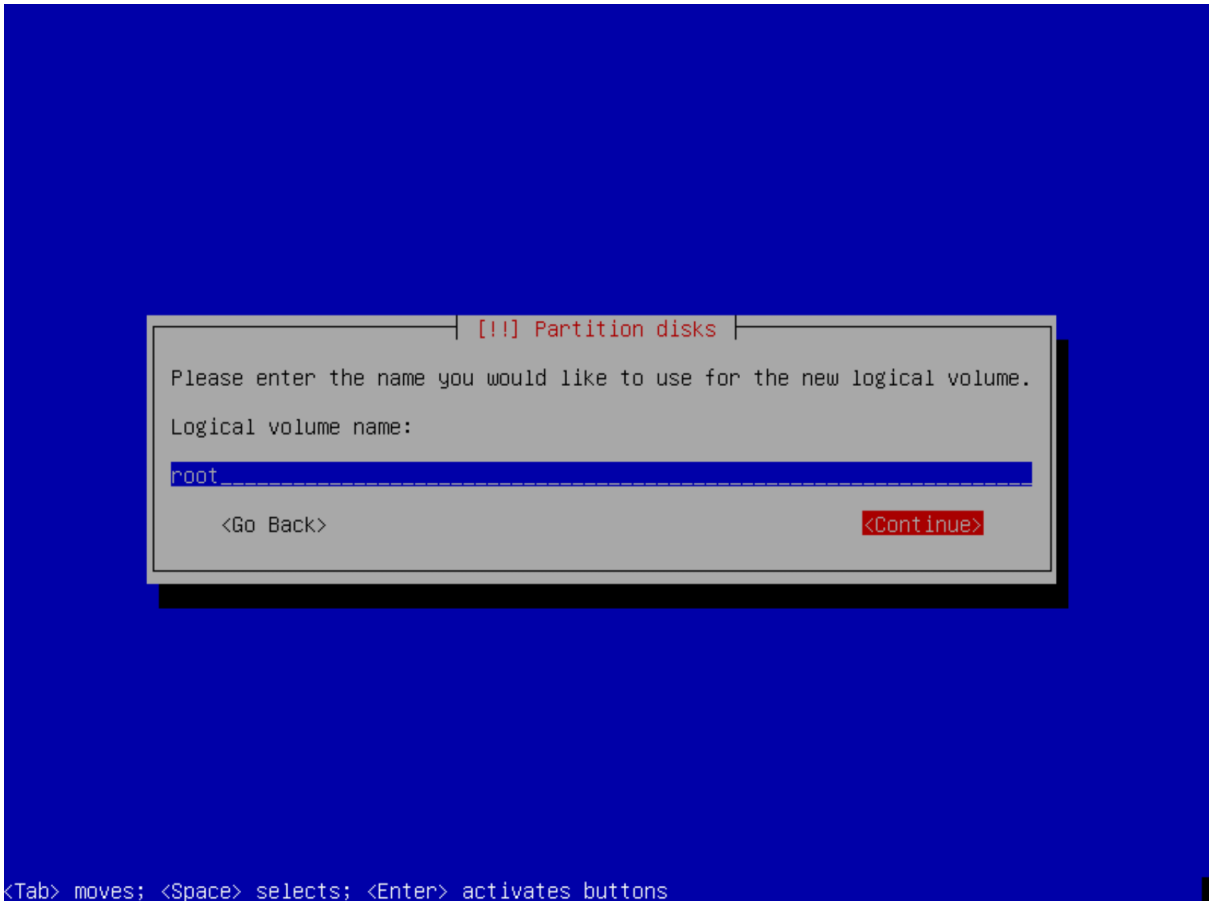
Select the encrypted partition.

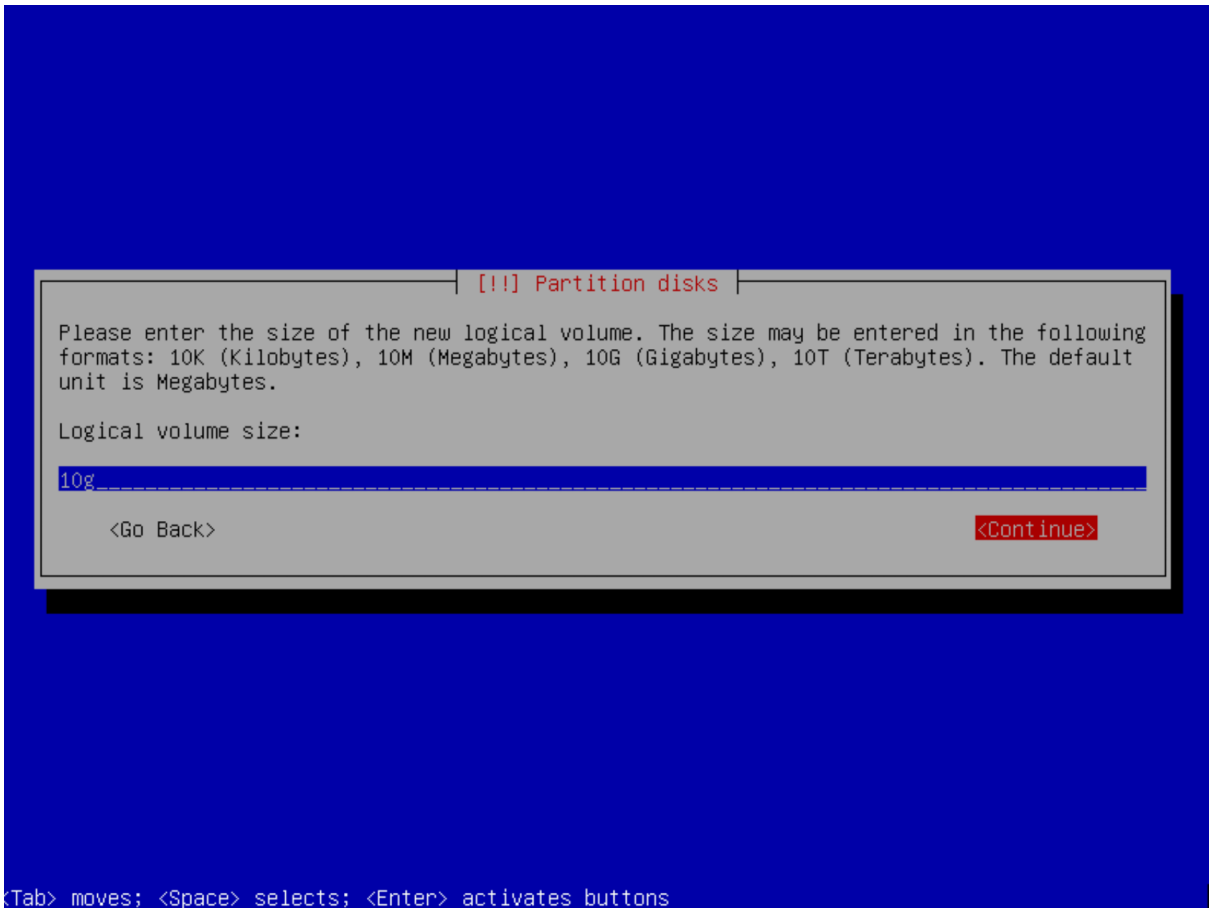


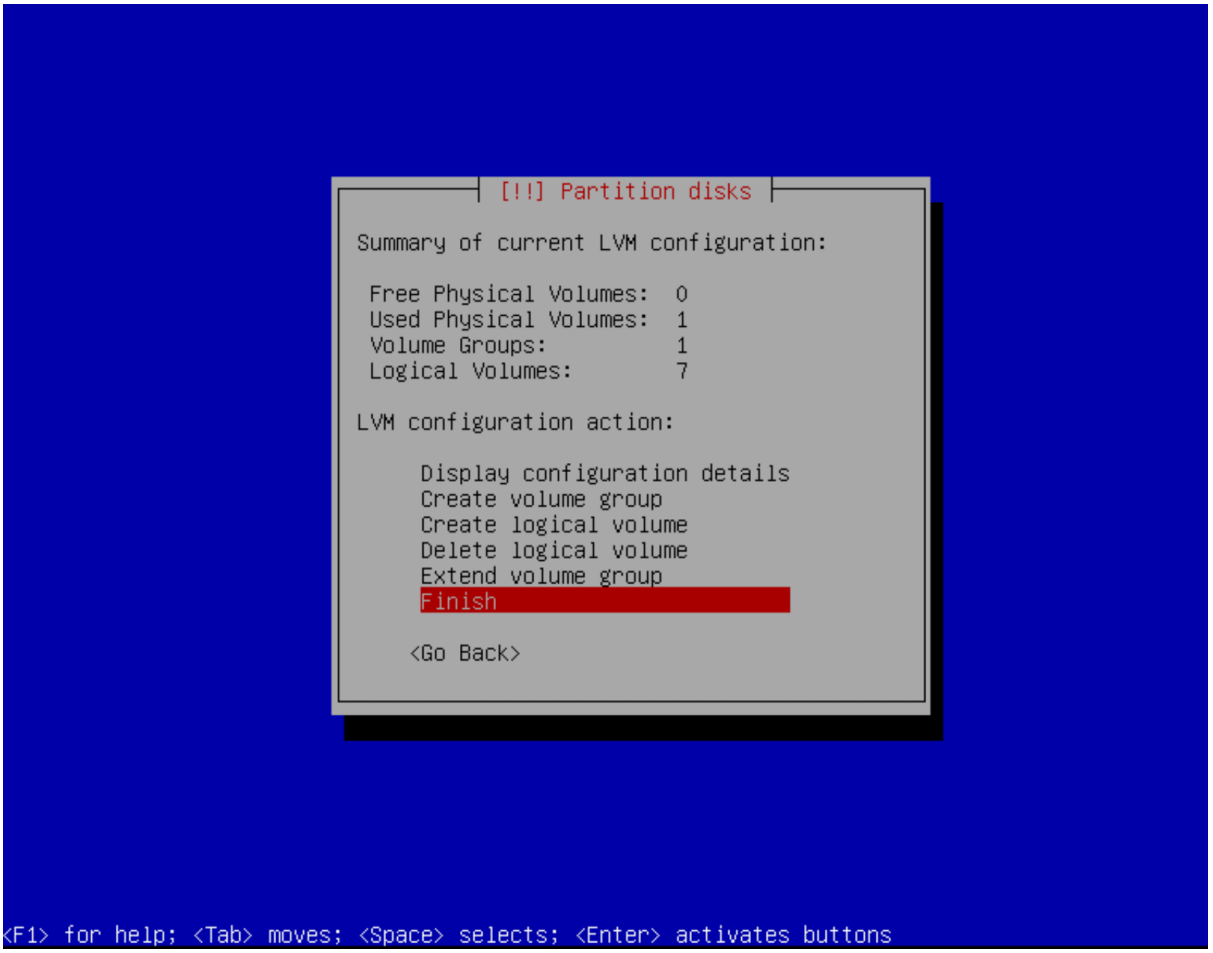
The following partitions will be created the same way but changing the size and the mount point. The exception is “swap” logical partition. For the amount of memory needed, see the subject instructions.

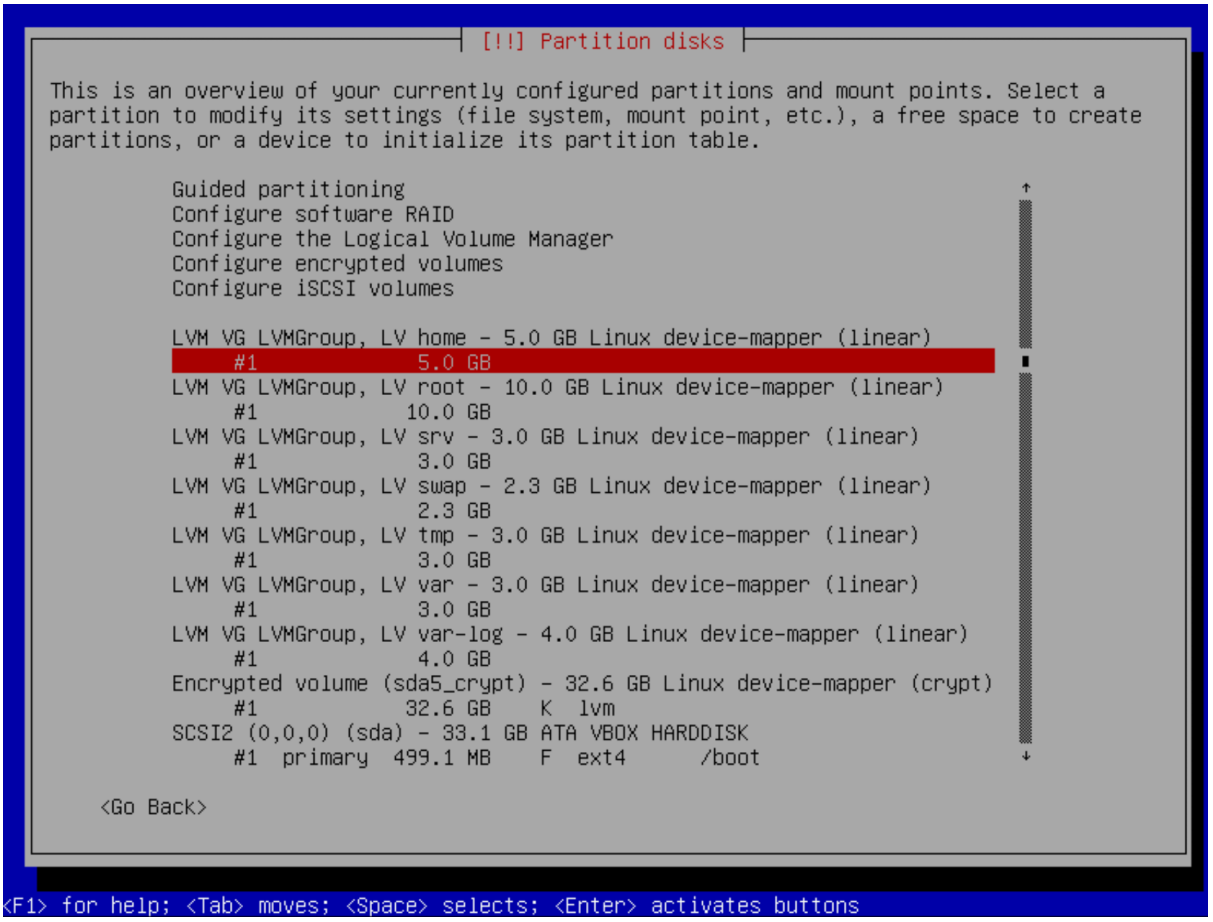

[!!] Partition disks
Summary of current LVM configuration:
Free Physical Volumes: 0
Used Physical Volumes: 1
Volume Groups: 1
Logical Volumes: 0
LVM configuration action:
Display configuration details
Create volume group
Create logical volume
Delete volume group
Extend volume group
Finish
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

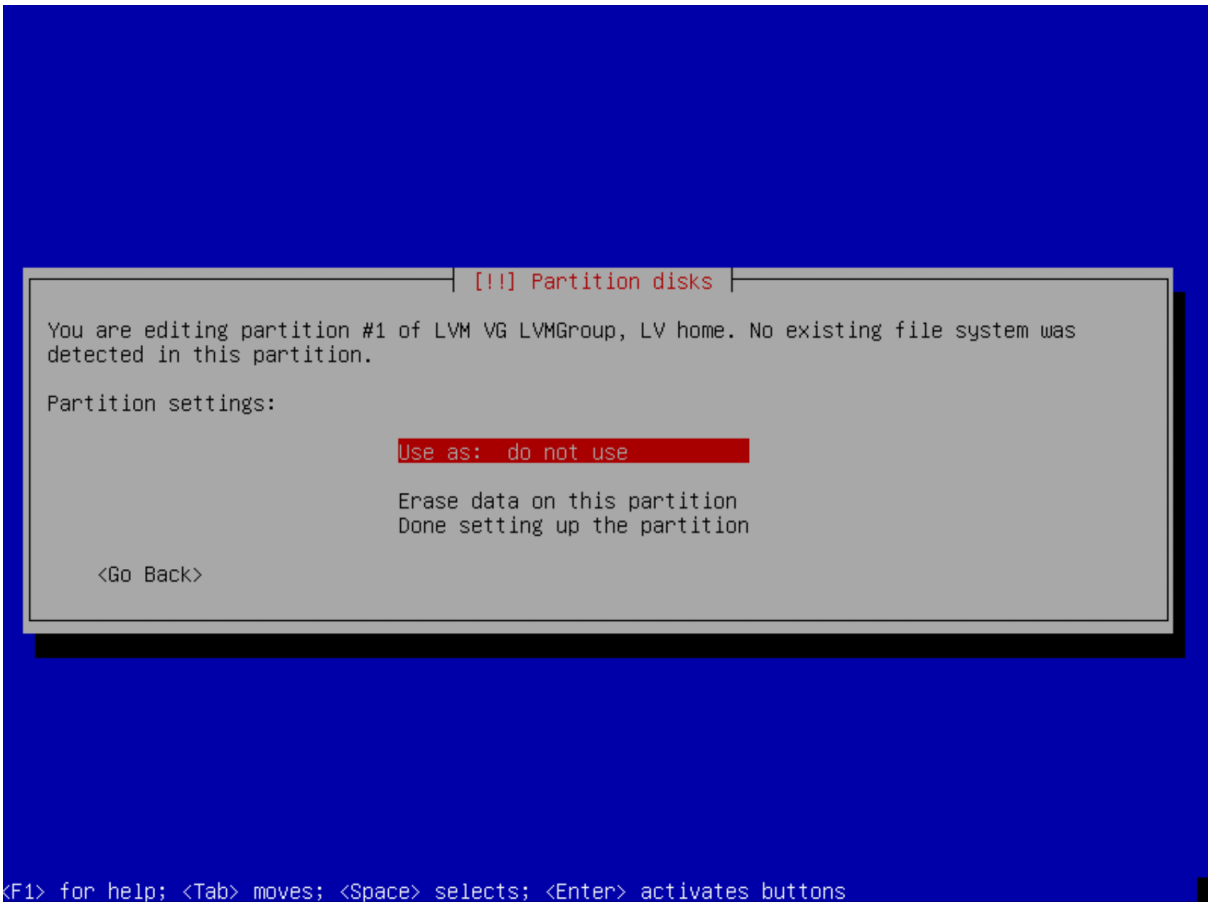

[!!] Partition disks
Please select the volume group where the new logical volume should be created.
Volume group:
LVMGroup (32551MB)
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

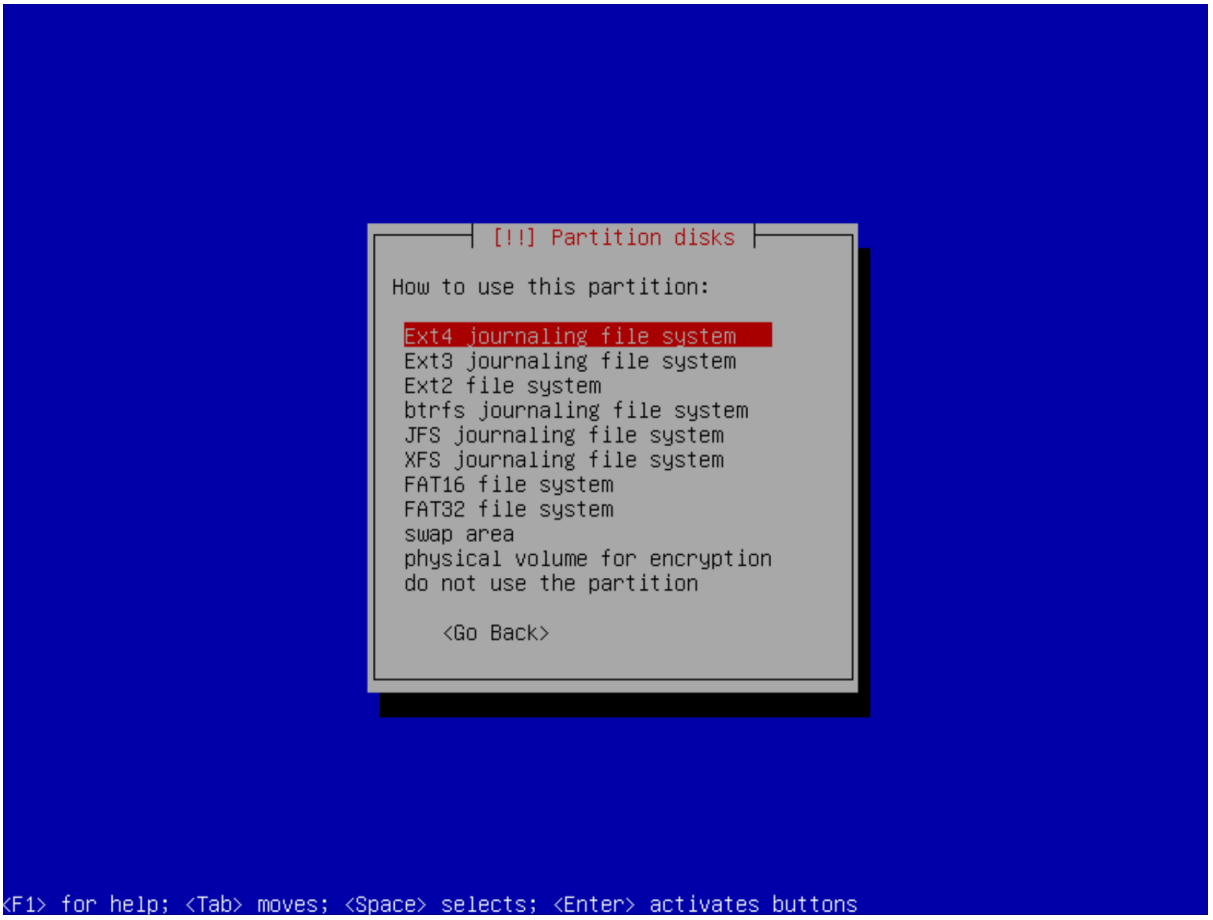

[!!] Partition disks
Please enter the name you would like to use for the new logical volume.
Logical volume name:
root
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

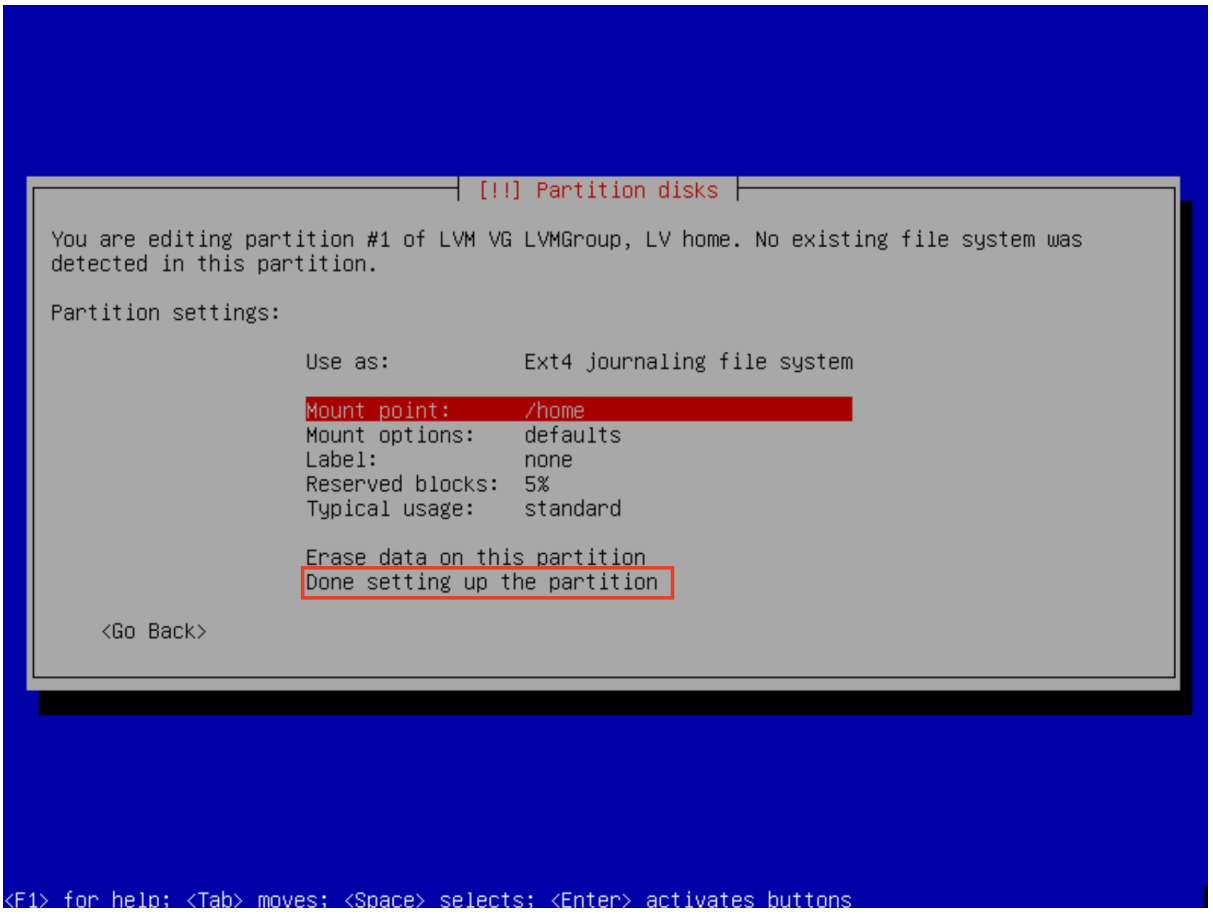

[!!] Partition disks
Please enter the size of the new logical volume. The size may be entered in the following formats: 10K (Kilobytes), 10M (Megabytes), 10G (Gigabytes), 10T (Terabytes). The default unit is Megabytes.
Logical volume size:
10g
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

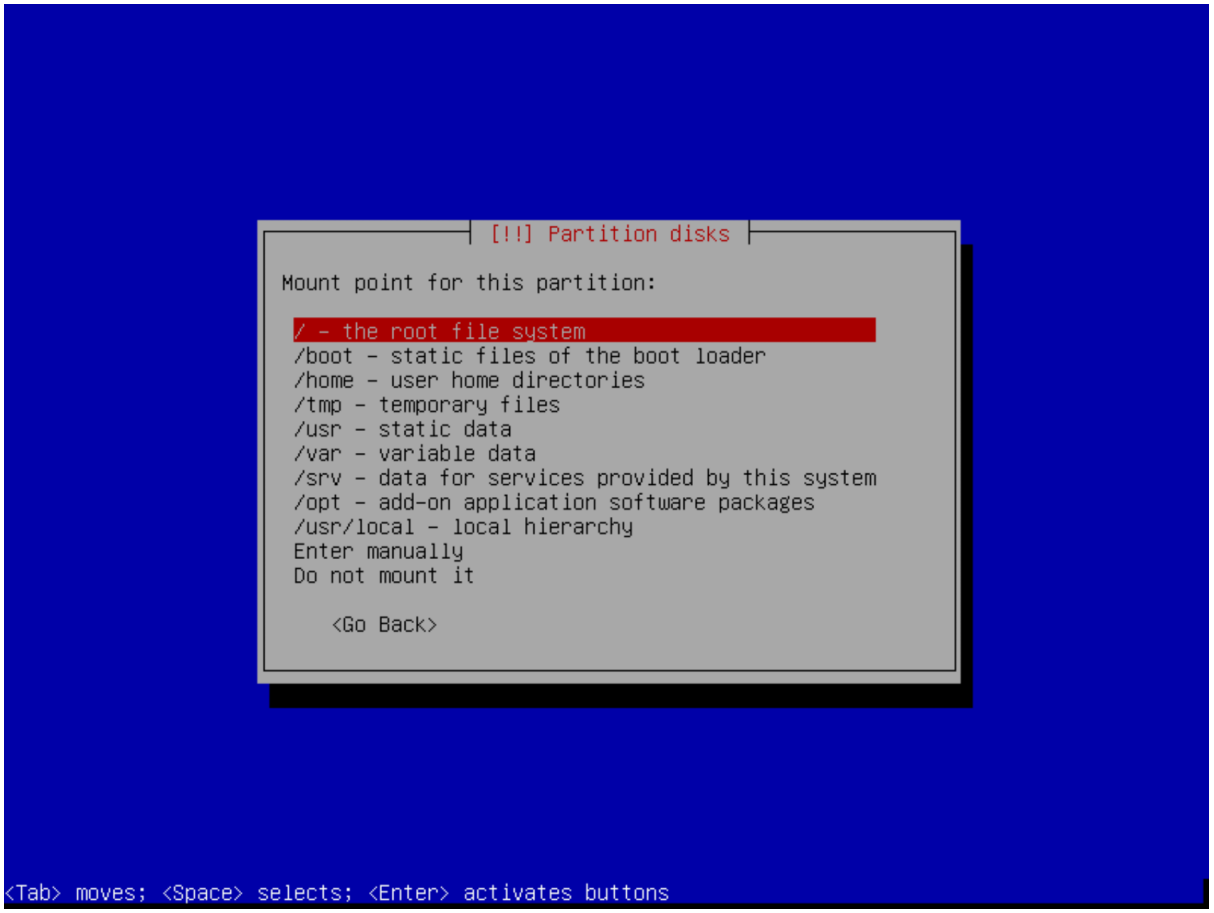

[!!] Partition disks
Summary of current LVM configuration:
Free Physical Volumes: 0
Used Physical Volumes: 1
Volume Groups: 1
Logical Volumes: 7
LVM configuration action:
Display configuration details
Create volume group
Create logical volume
Delete logical volume
Extend volume group
Finish
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

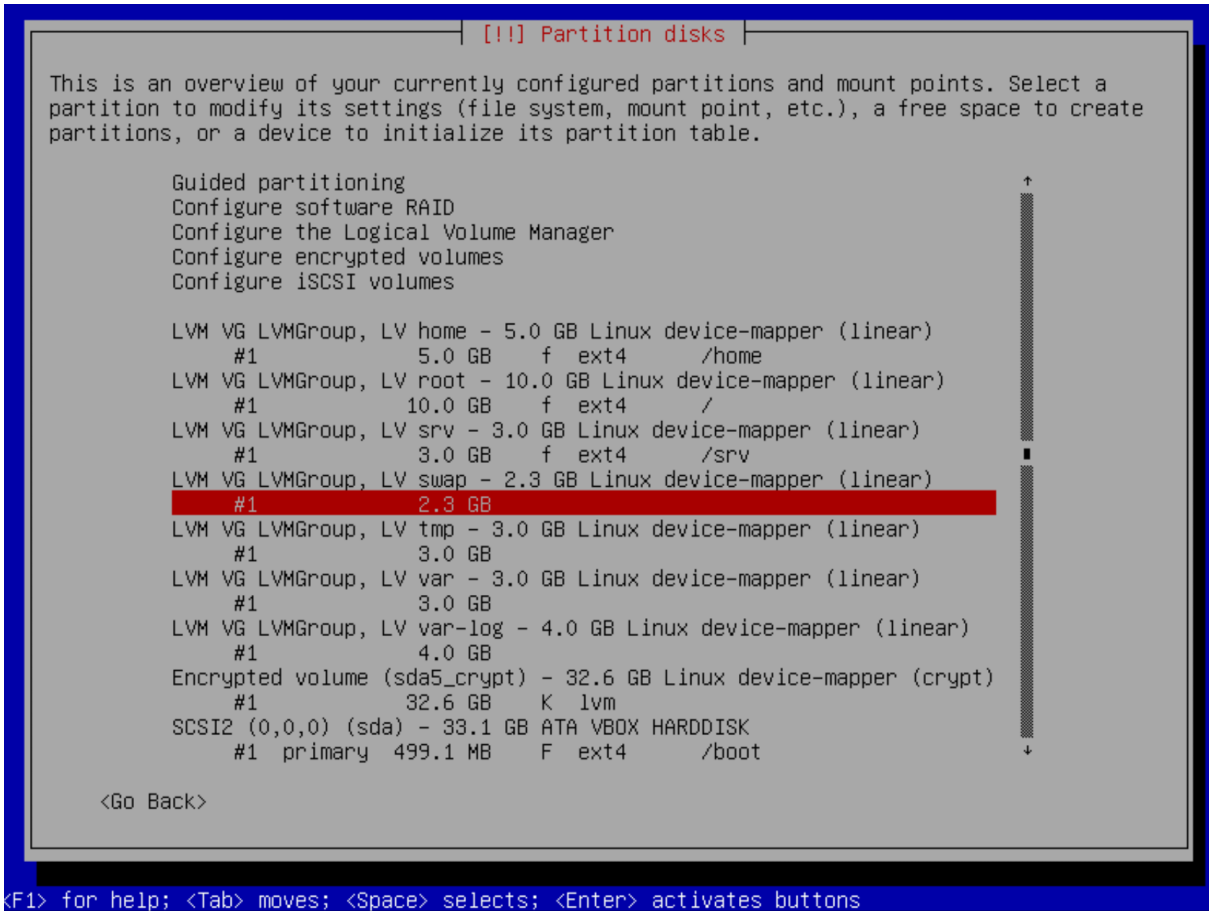

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
LVM VG LVMGroup, LV home - 5.0 GB Linux device-mapper (linear)
#1 5.0 GB
LVM VG LVMGroup, LV root - 10.0 GB Linux device-mapper (linear)
#1 10.0 GB
LVM VG LVMGroup, LV srv - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB
LVM VG LVMGroup, LV swap - 2.3 GB Linux device-mapper (linear)
#1 2.3 GB
LVM VG LVMGroup, LV tmp - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB
LVM VG LVMGroup, LV var - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB
LVM VG LVMGroup, LV var-log - 4.0 GB Linux device-mapper (linear)
#1 4.0 GB
Encrypted volume (sda5_crypt) - 32.6 GB Linux device-mapper (crypt)
#1 32.6 GB K lvm
SCSI2 (0,0,0) (sda) - 33.1 GB ATA VBOX HARDDISK
#1 primary 499.1 MB F ext4 /boot
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Partition disks
You are editing partition #1 of LVM VG LVMGroup, LV home. No existing file system was detected in this partition.
Partition settings:
Use as: do not use
Erase data on this partition
Done setting up the partition
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

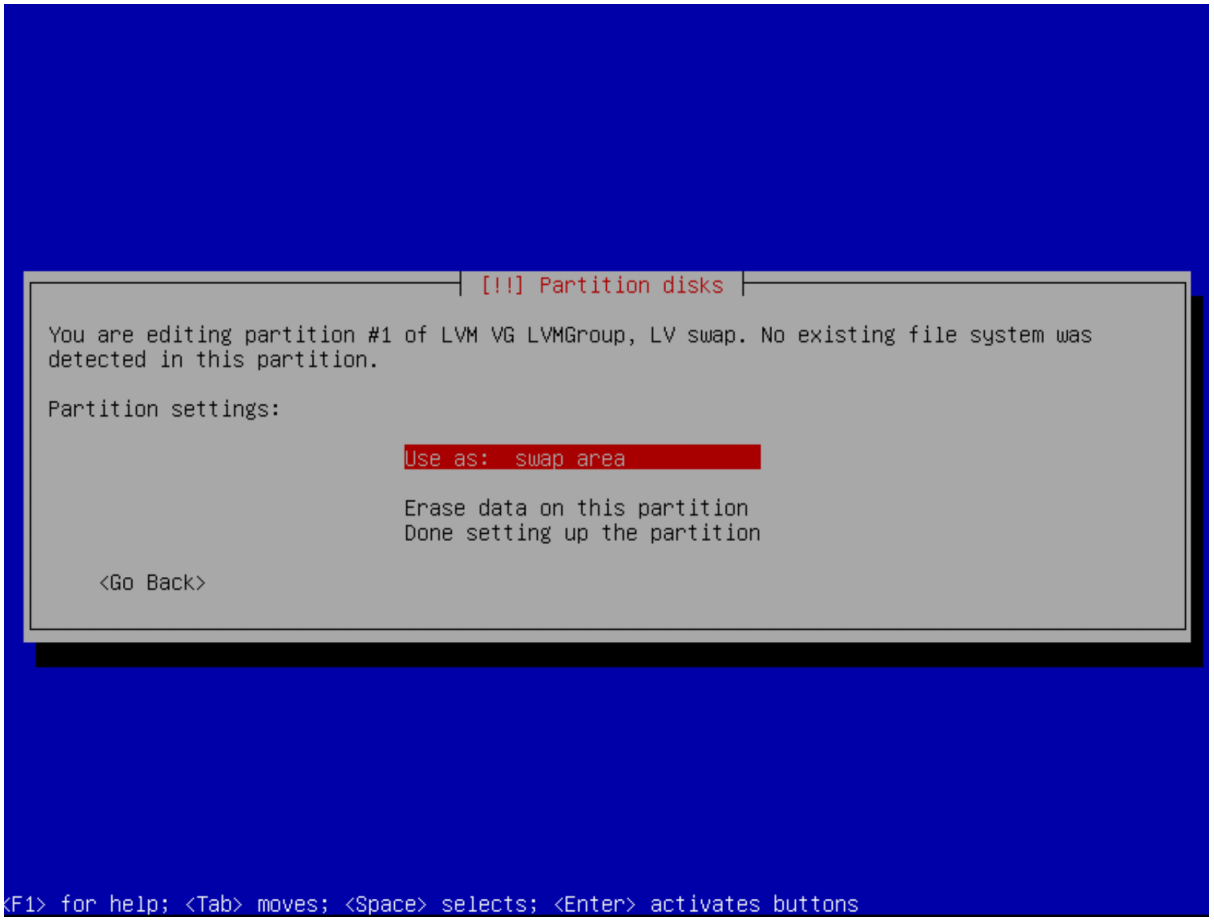

[!!] Partition disks
How to use this partition:
Ext4 journaling file system
Ext3 journaling file system
Ext2 file system
btrfs journaling file system
JFS journaling file system
XFS journaling file system
FAT16 file system
FAT32 file system
swap area
physical volume for encryption
do not use the partition
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

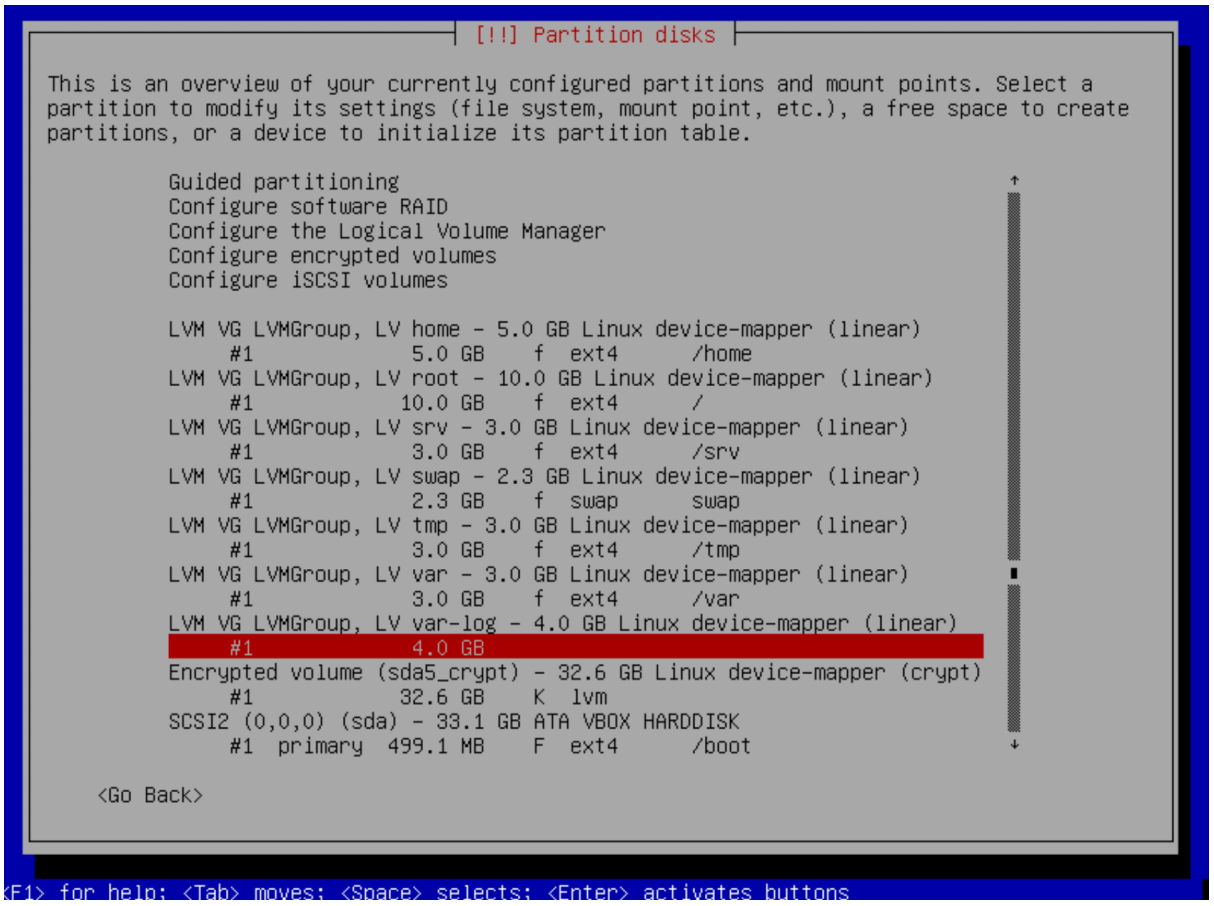

[!!] Partition disks
You are editing partition #1 of LVM VG LVMGroup, LV home. No existing file system was detected in this partition.
Partition settings:
Use as: Ext4 journaling file system
Mount point: /home
Mount options: defaults
Label: none
Reserved blocks: 5%
Typical usage: standard
Erase data on this partition
Done setting up the partition
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

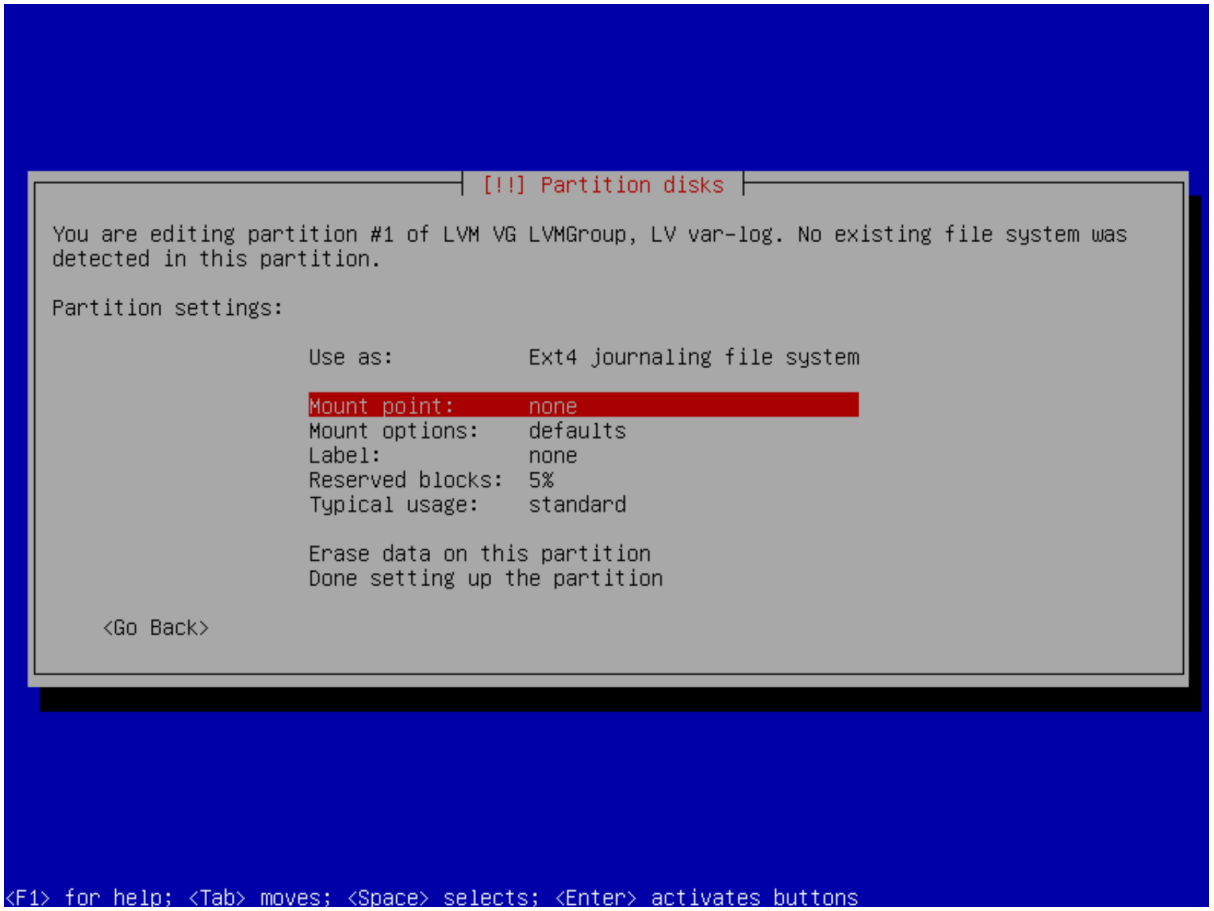

[!!] Partition disks
Mount point for this partition:
/ - the root file system
/boot - static files of the boot loader
/home - user home directories
/tmp - temporary files
/usr - static data
/var - variable data
/srv - data for services provided by this system
/opt - add-on application software packages
/usr/local - local hierarchy
Enter manually
Do not mount it
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

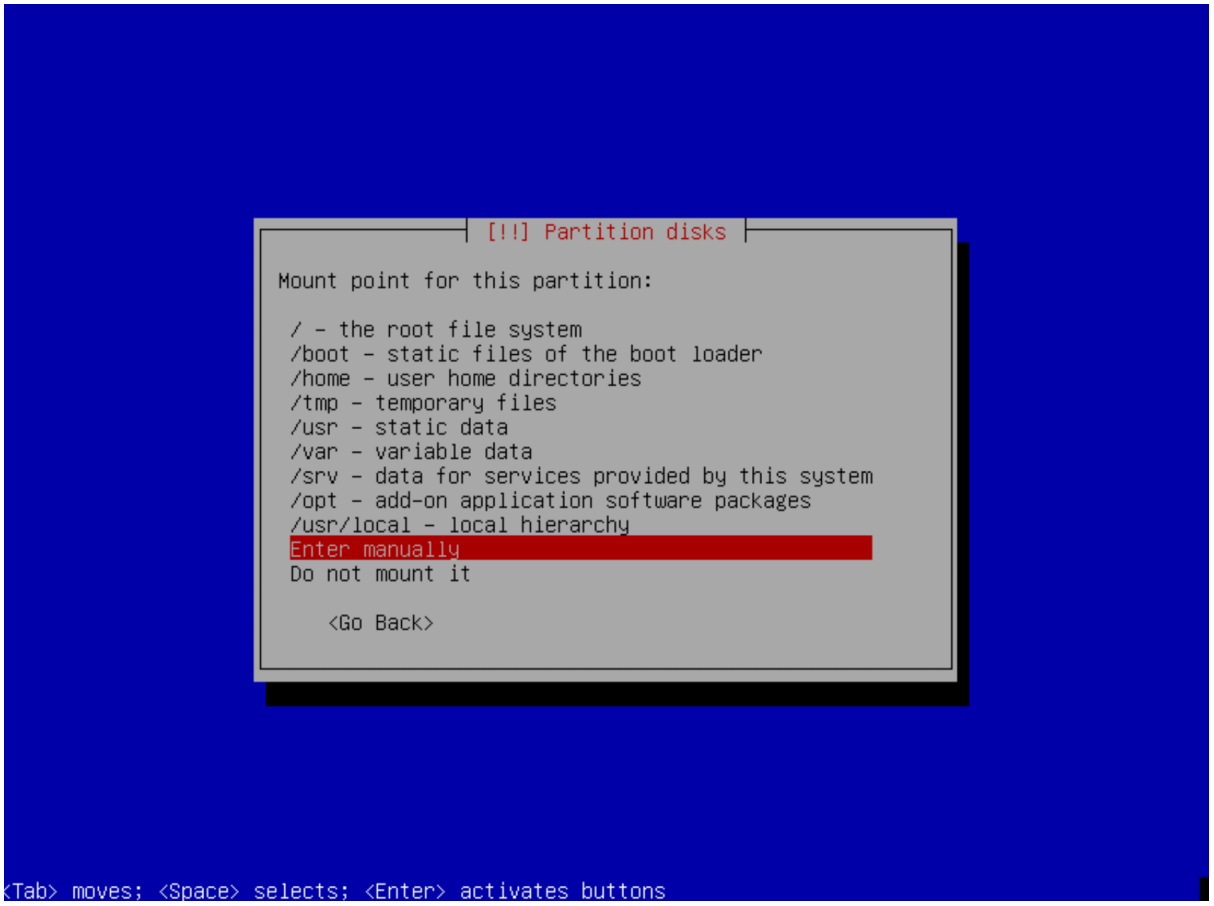

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
LVM VG LVMGroup, LV home - 5.0 GB Linux device-mapper (linear)
#1 5.0 GB f ext4 /home
LVM VG LVMGroup, LV root - 10.0 GB Linux device-mapper (linear)
#1 10.0 GB f ext4 /
LVM VG LVMGroup, LV srv - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB f ext4 /srv
LVM VG LVMGroup, LV swap - 2.3 GB Linux device-mapper (linear)
#1 2.3 GB
LVM VG LVMGroup, LV tmp - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB
LVM VG LVMGroup, LV var - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB
LVM VG LVMGroup, LV var-log - 4.0 GB Linux device-mapper (linear)
#1 4.0 GB
Encrypted volume (sda5_crypt) - 32.6 GB Linux device-mapper (crypt)
#1 32.6 GB K lvm
SCSI2 (0,0,0) (sda) - 33.1 GB ATA VBOX HARDDISK
#1 primary 499.1 MB F ext4 /boot
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

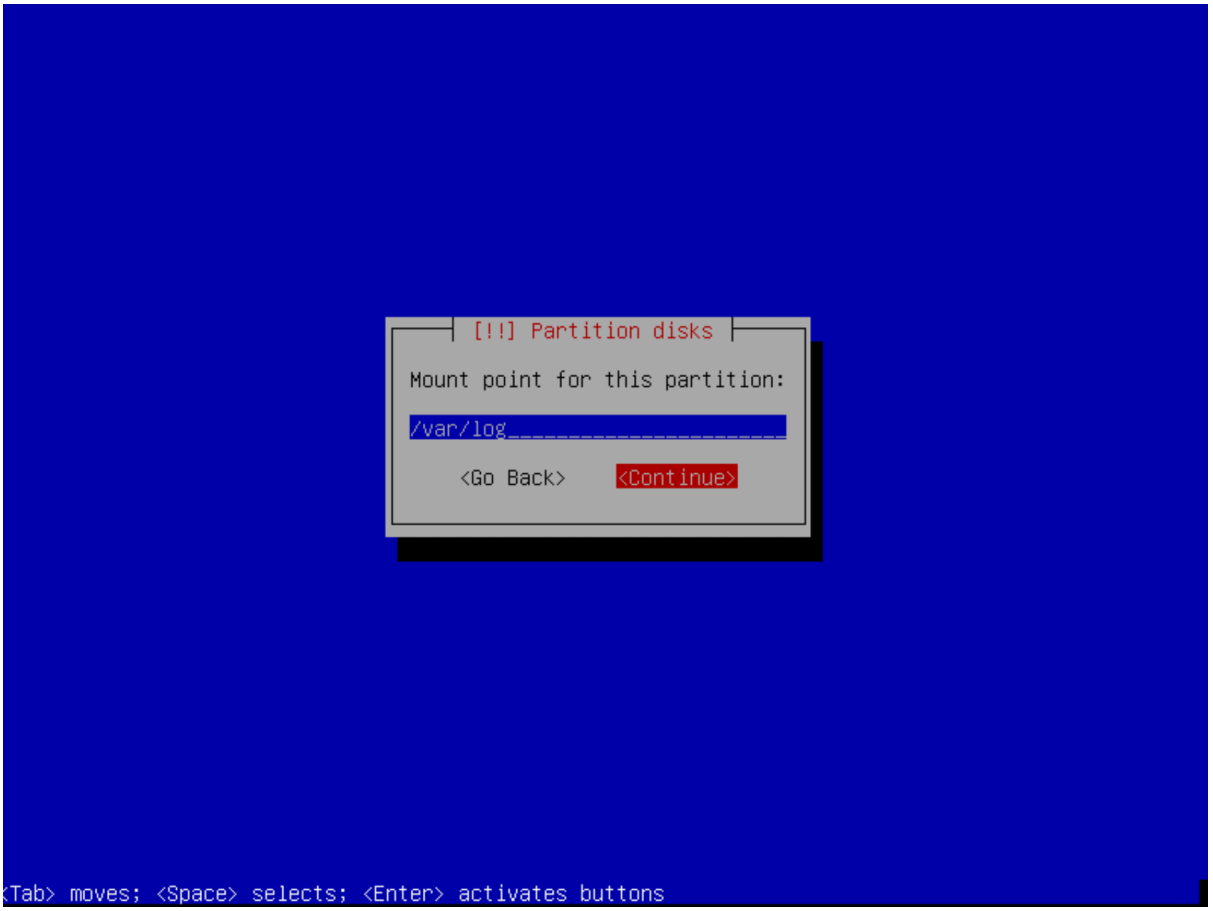
The swap partition is a special one, because it will be used as virtual RAM.

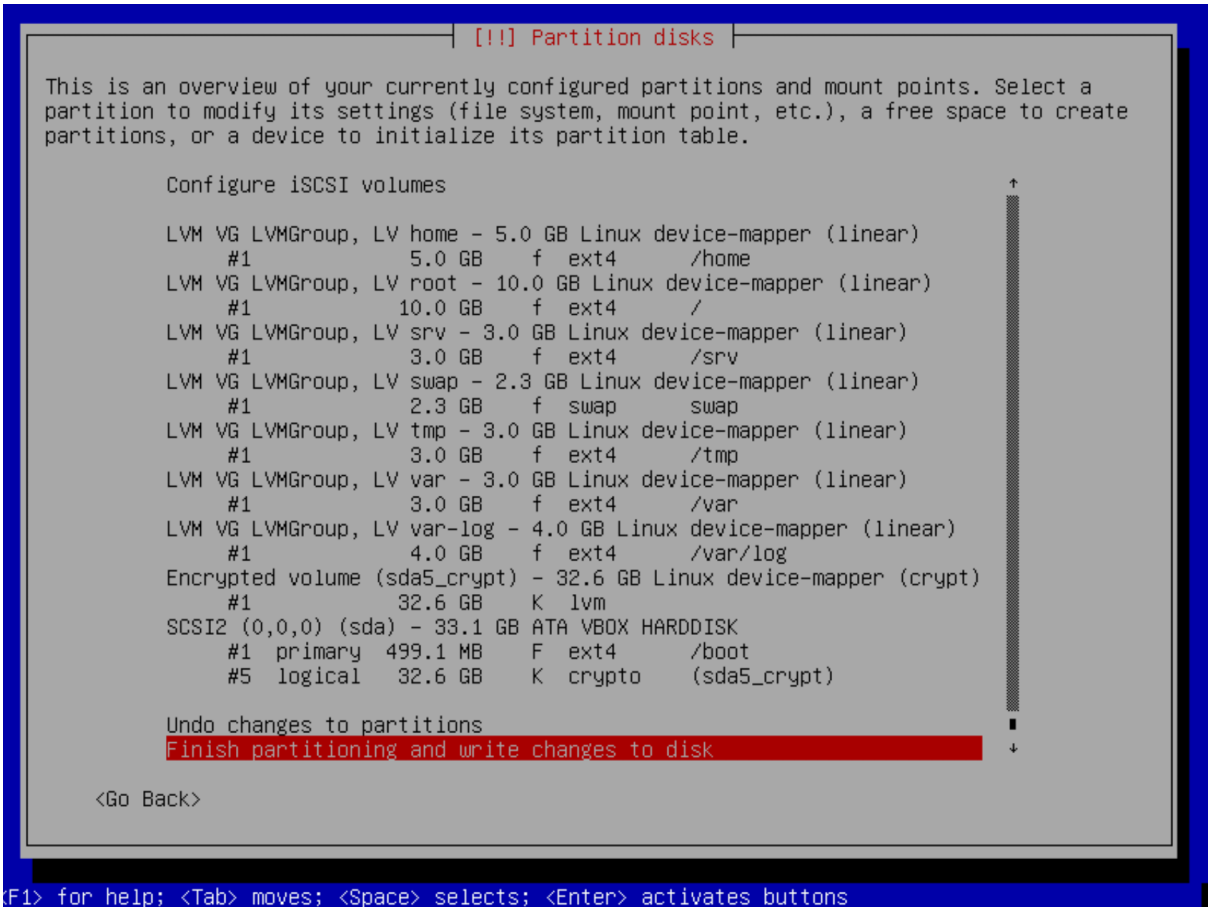

[!!] Partition disks
You are editing partition #1 of LVM VG LVMGroup, LV swap. No existing file system was detected in this partition.
Partition settings:
Use as: swap area
Erase data on this partition
Done setting up the partition
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

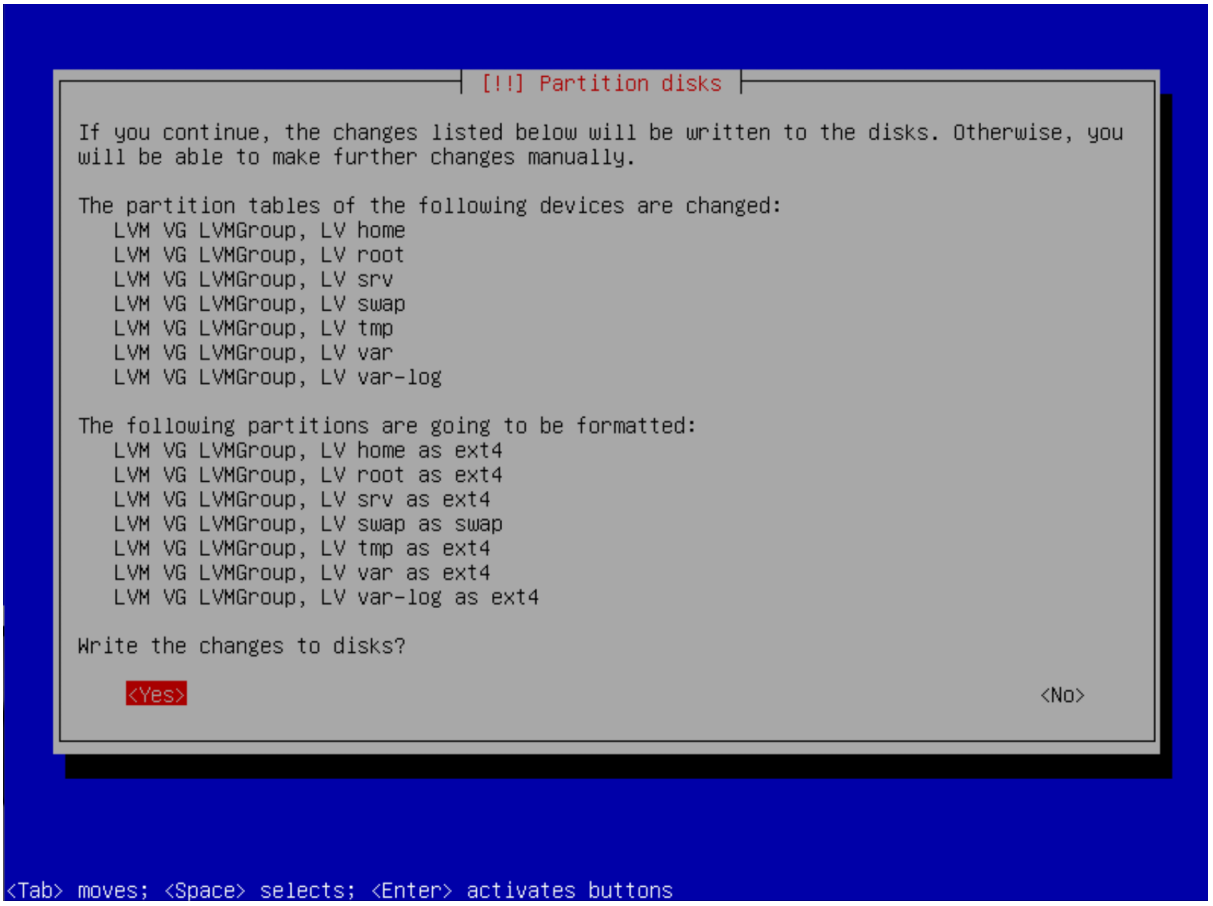

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
LVM VG LVMGroup, LV home - 5.0 GB Linux device-mapper (linear)
#1 5.0 GB f ext4 /home
LVM VG LVMGroup, LV root - 10.0 GB Linux device-mapper (linear)
#1 10.0 GB f ext4 /
LVM VG LVMGroup, LV srv - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB f ext4 /srv
LVM VG LVMGroup, LV swap - 2.3 GB Linux device-mapper (linear)
#1 2.3 GB f swap swap
LVM VG LVMGroup, LV tmp - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB f ext4 /tmp
LVM VG LVMGroup, LV var - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB f ext4 /var
LVM VG LVMGroup, LV var-log - 4.0 GB Linux device-mapper (linear)
#1 4.0 GB
Encrypted volume (sda5_crypt) - 32.6 GB Linux device-mapper (crypt)
#1 32.6 GB K lvm
SCSI2 (0,0,0) (sda) - 33.1 GB ATA VBOX HARDDISK
#1 primary 499.1 MB F ext4 /boot
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Partition disks
You are editing partition #1 of LVM VG LVMGroup, LV var-log. No existing file system was detected in this partition.
Partition settings:
Use as: Ext4 journaling file system
Mount point: none
Mount options: defaults
Label: none
Reserved blocks: 5%
Typical usage: standard
Erase data on this partition
Done setting up the partition
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

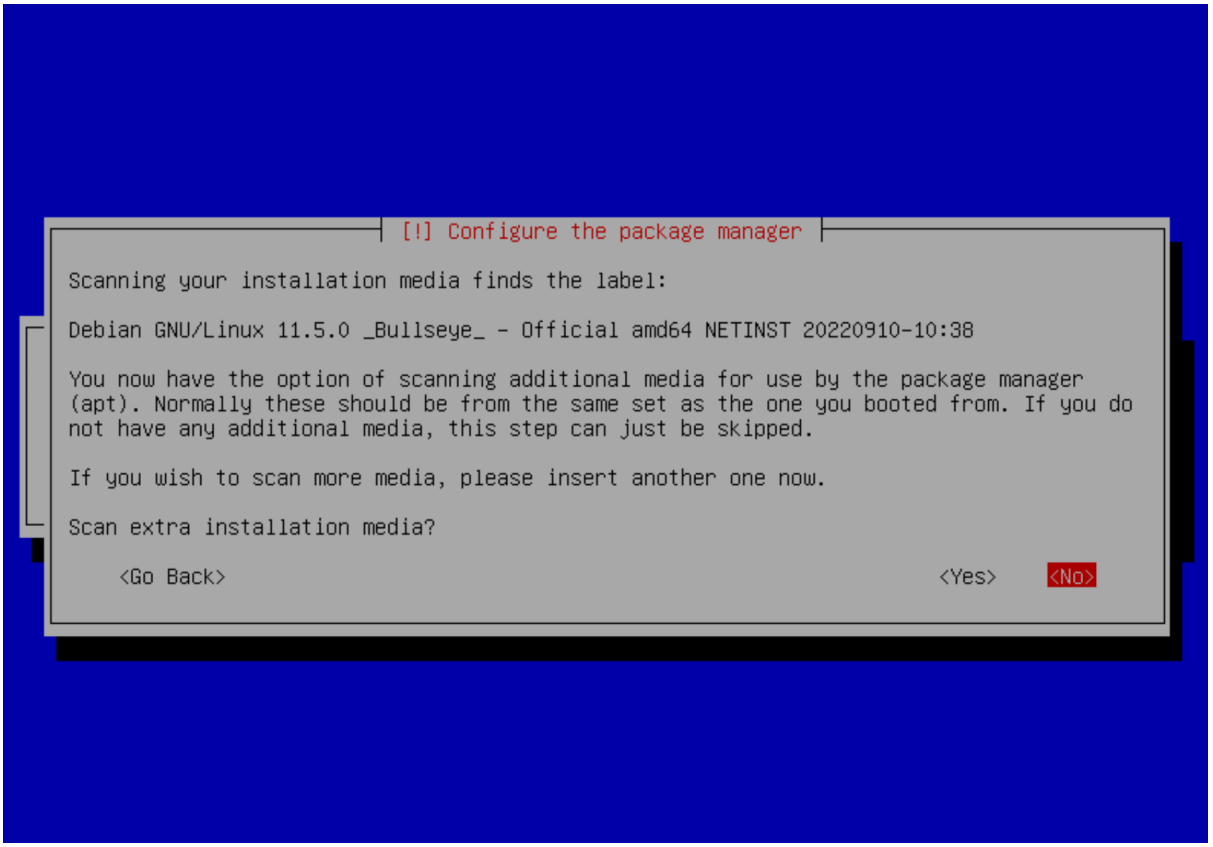

[!!] Partition disks
Mount point for this partition:
/ - the root file system
/boot - static files of the boot loader
/home - user home directories
/tmp - temporary files
/usr - static data
/var - variable data
/srv - data for services provided by this system
/opt - add-on application software packages
/usr/local - local hierarchy
Enter manually
Do not mount it
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

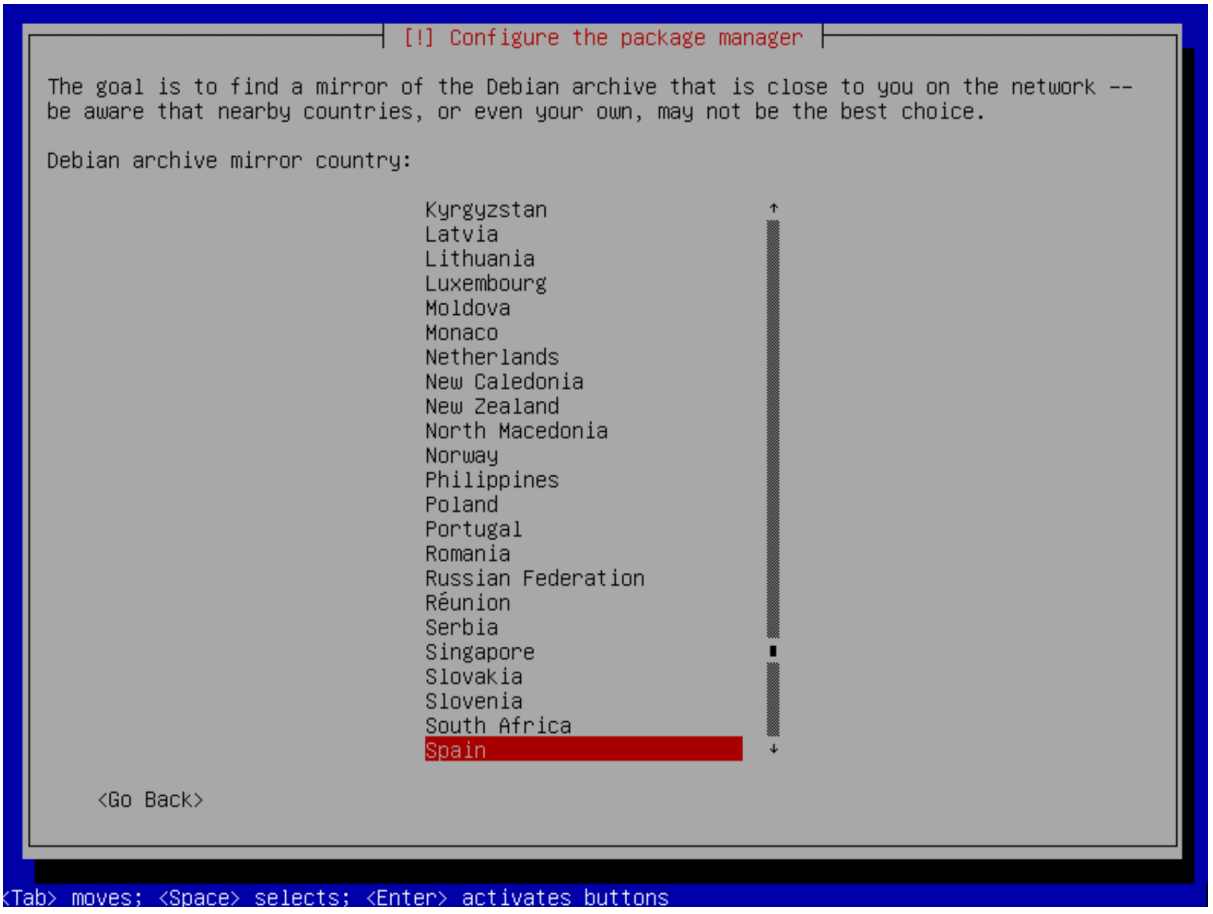

[!!] Partition disks
Mount point for this partition:
/var/log
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

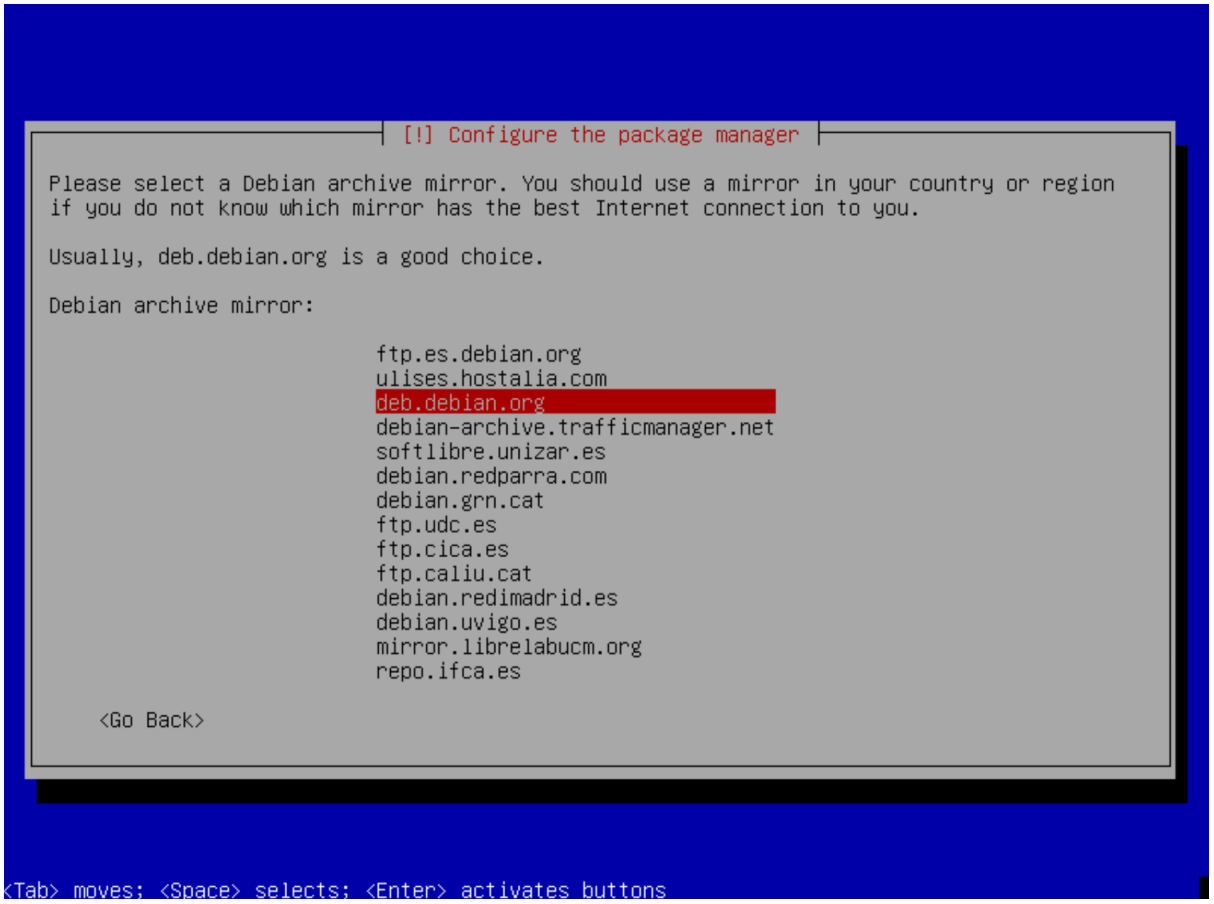

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Configure iSCSI volumes
LVM VG LVMGroup, LV home - 5.0 GB Linux device-mapper (linear)
#1 5.0 GB f ext4 /home
LVM VG LVMGroup, LV root - 10.0 GB Linux device-mapper (linear)
#1 10.0 GB f ext4 /
LVM VG LVMGroup, LV srv - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB f ext4 /srv
LVM VG LVMGroup, LV swap - 2.3 GB Linux device-mapper (linear)
#1 2.3 GB f swap swap
LVM VG LVMGroup, LV tmp - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB f ext4 /tmp
LVM VG LVMGroup, LV var - 3.0 GB Linux device-mapper (linear)
#1 3.0 GB f ext4 /var
LVM VG LVMGroup, LV var-log - 4.0 GB Linux device-mapper (linear)
#1 4.0 GB f ext4 /var/log
Encrypted volume (sda5_crypt) - 32.6 GB Linux device-mapper (crypt)
#1 32.6 GB K lvm
SCSI2 (0,0,0) (sda) - 33.1 GB ATA VBOX HARDDISK
#1 primary 499.1 MB F ext4 /boot
#5 logical 32.6 GB K crypto (sda5_crypt)
Undo changes to partitions
Finish partitioning and write changes to disk
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

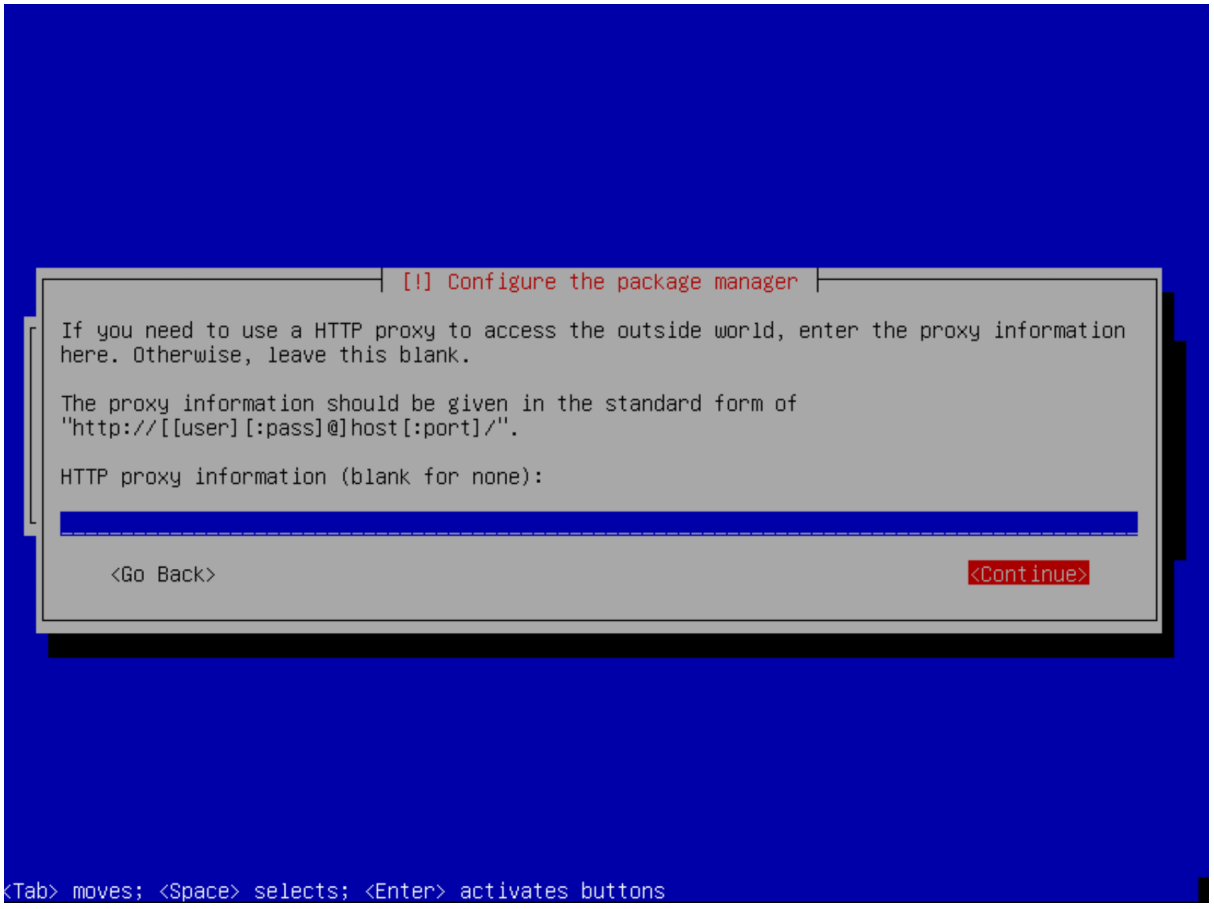

[!!] Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
LVM VG LVMGroup, LV home
LVM VG LVMGroup, LV root
LVM VG LVMGroup, LV srv
LVM VG LVMGroup, LV swap
LVM VG LVMGroup, LV tmp
LVM VG LVMGroup, LV var
LVM VG LVMGroup, LV var-log
The following partitions are going to be formatted:
LVM VG LVMGroup, LV home as ext4
LVM VG LVMGroup, LV root as ext4
LVM VG LVMGroup, LV srv as ext4
LVM VG LVMGroup, LV swap as swap
LVM VG LVMGroup, LV tmp as ext4
LVM VG LVMGroup, LV var as ext4
LVM VG LVMGroup, LV var-log as ext4
Write the changes to disks?
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons

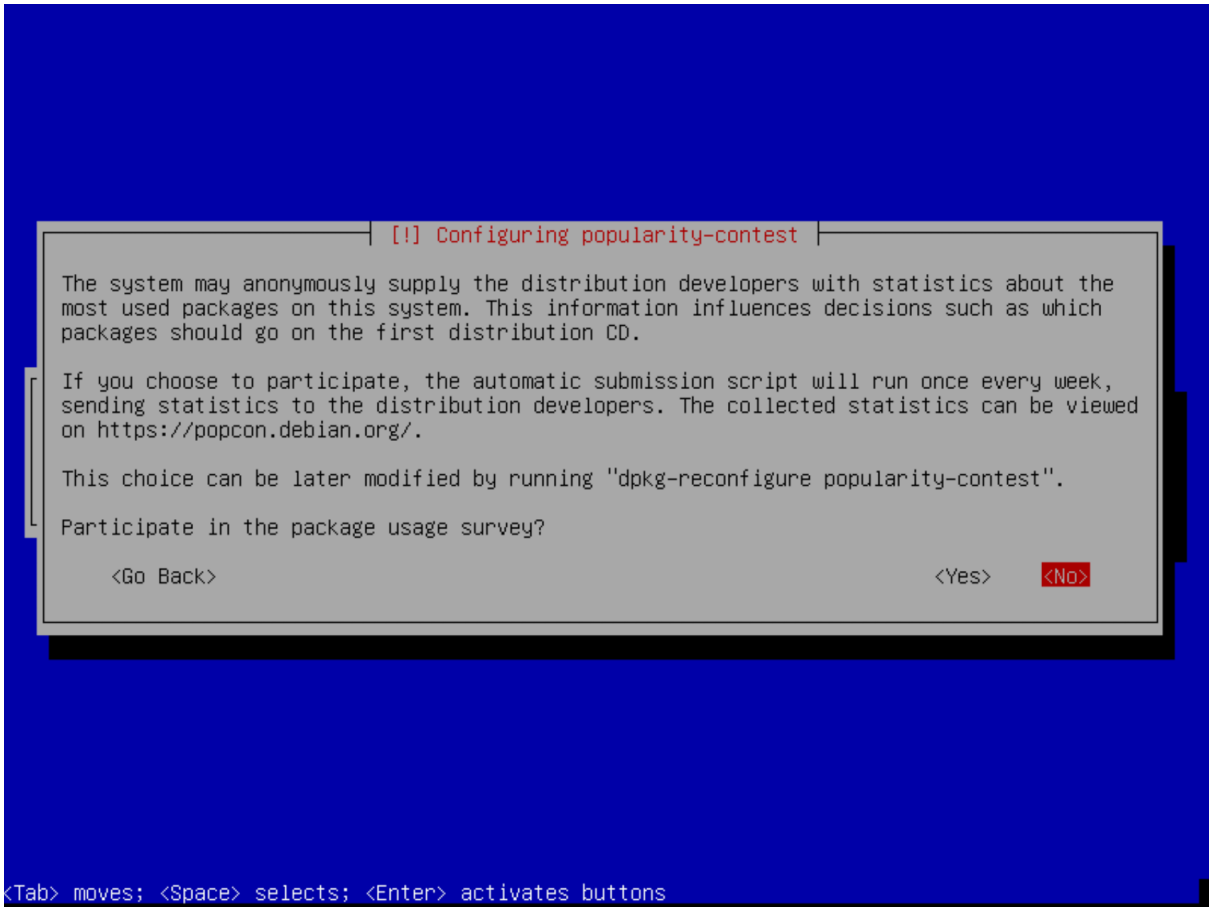
All the partitions are correctly configured now. Now it asks us to configure the package manager. I selected my country for better speed downloading the packages.



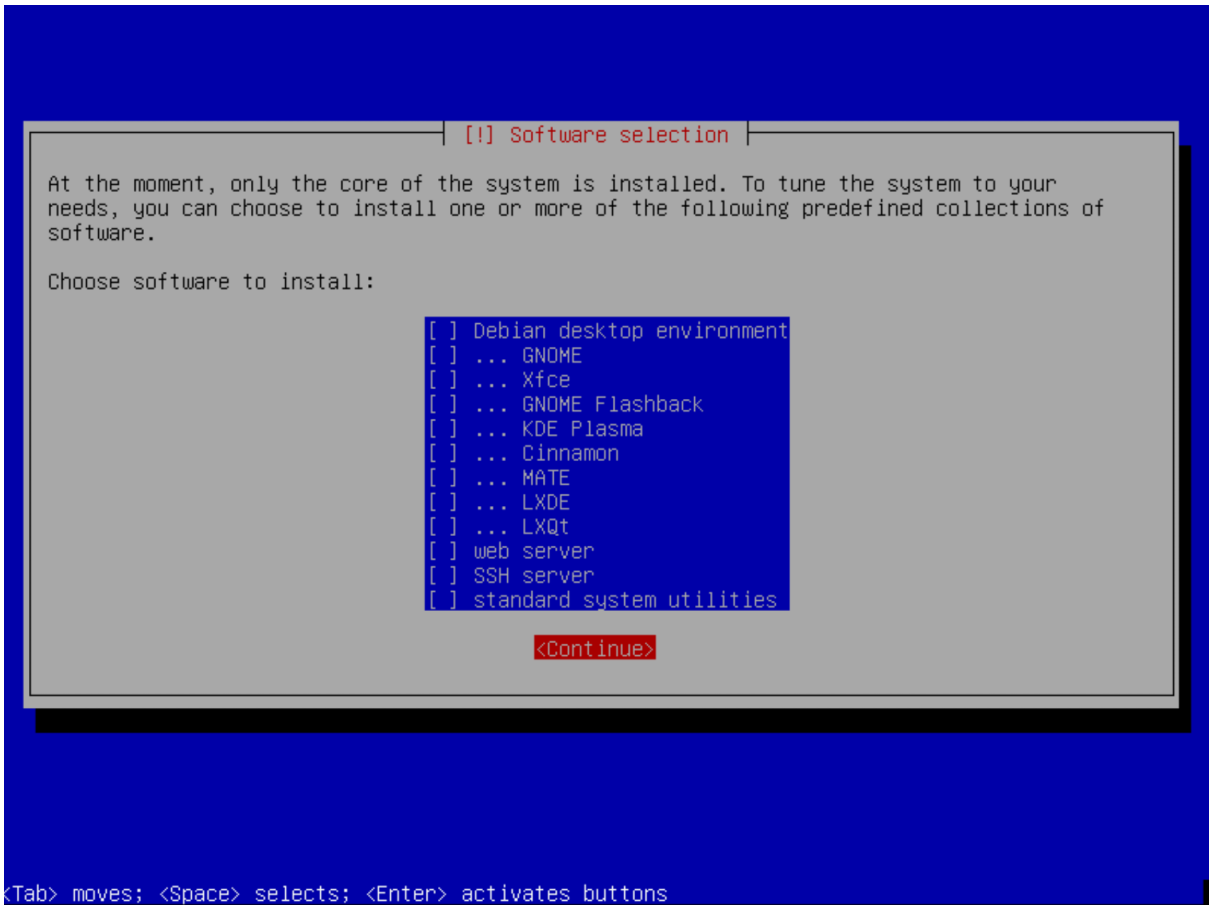



[!] Configure the package manager
Please select a Debian archive mirror. You should use a mirror in your country or region
if you do not know which mirror has the best Internet connection to you.
Usually, deb.debian.org is a good choice.
Debian archive mirror:
ftp.es.debian.org
ulises.hostalia.com
deb.debian.org
debian-archive.trafficmanager.net
softlibre.unizar.es
debian.redparra.com
debian.grn.cat
ftp.udc.es
ftp.cica.es
ftp.caliu.cat
debian.redimadrid.es
debian.uvigo.es
mirror.librelabucm.org
repo.ifca.es
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

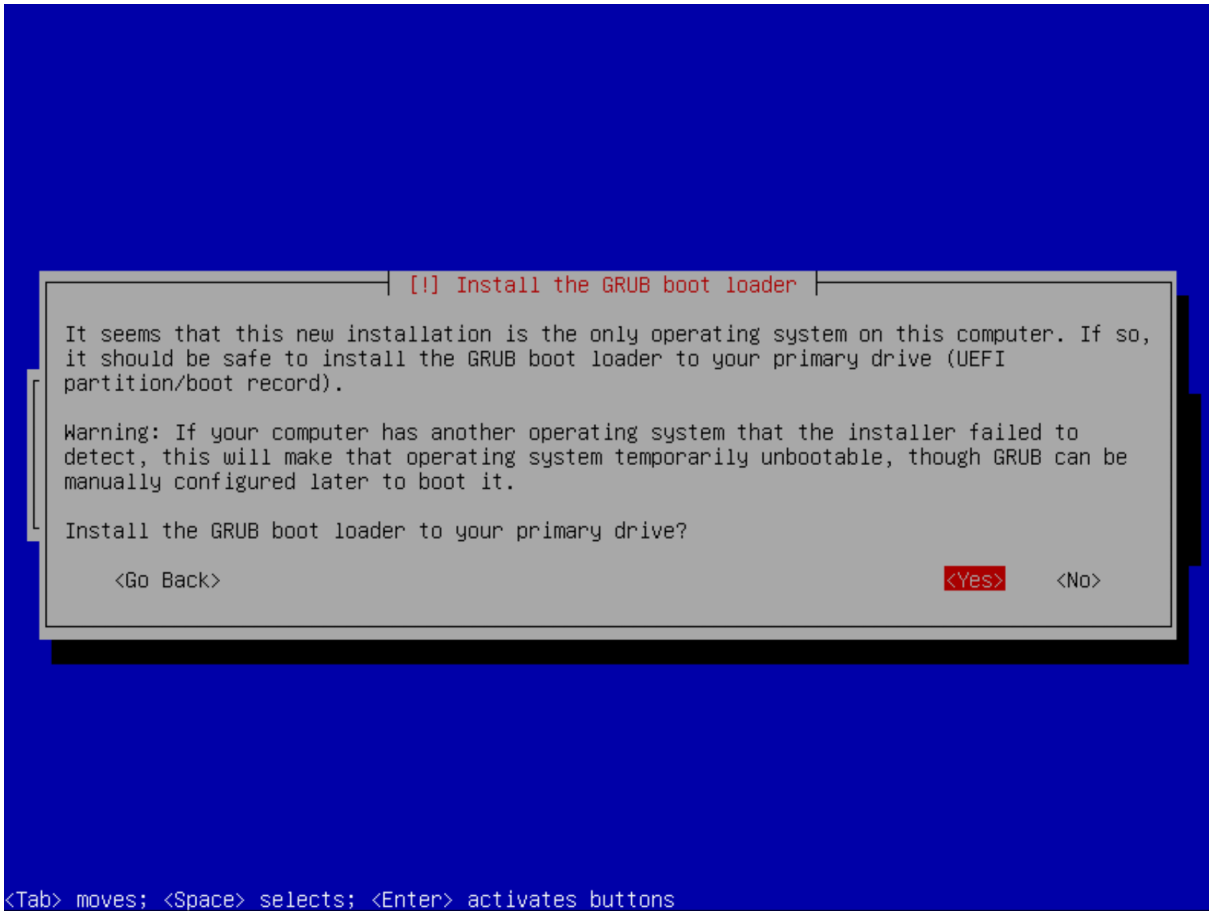

[!] Configure the package manager
If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".
HTTP proxy information (blank for none):
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

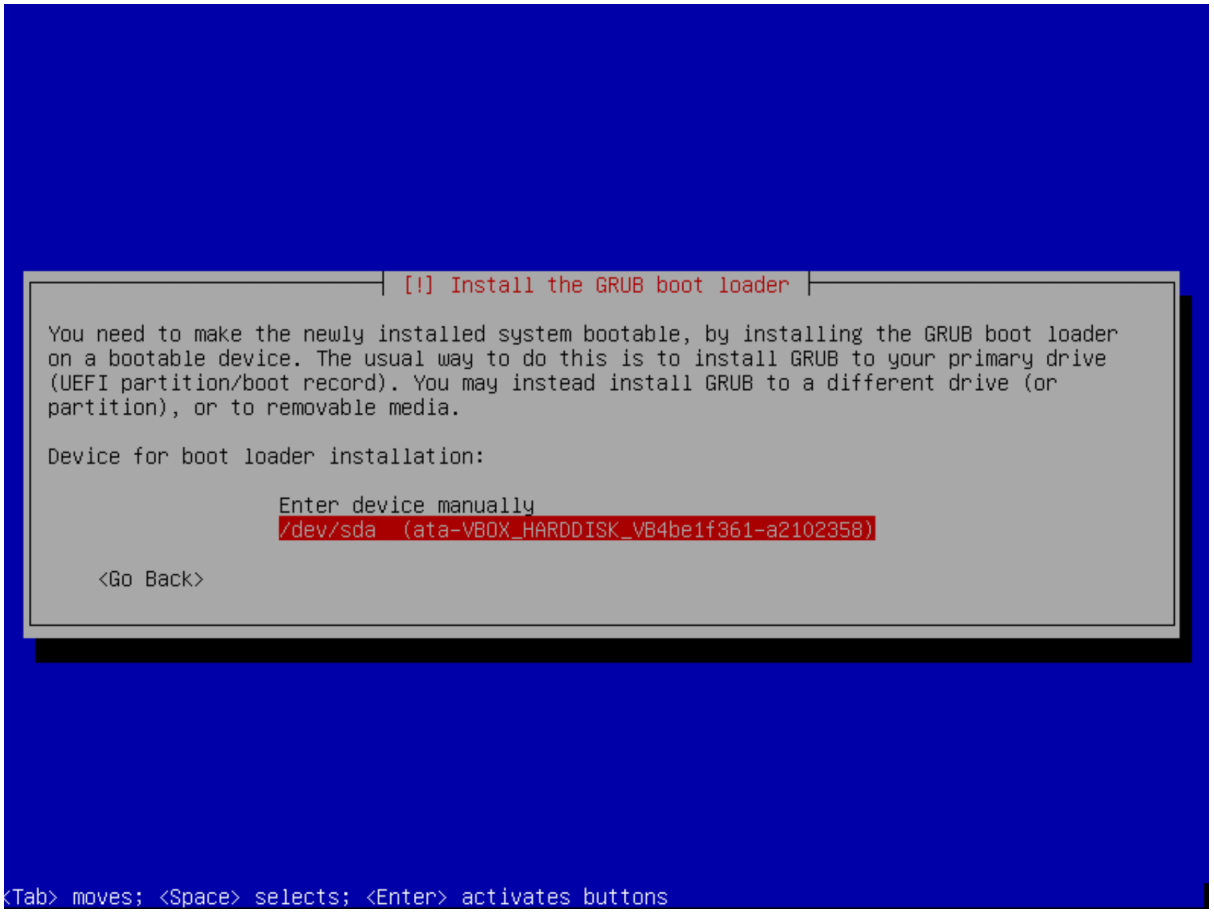

[!] Configuring popularity-contest
The system may anonymously supply the distribution developers with statistics about the most used packages on this system. This information influences decisions such as which packages should go on the first distribution CD.
If you choose to participate, the automatic submission script will run once every week, sending statistics to the distribution developers. The collected statistics can be viewed on https://popcon.debian.org/.
This choice can be later modified by running "dpkg-reconfigure popularity-contest".
Participate in the package usage survey?
<Go Back>
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons

We don’t want extra software so uncheck all the boxes.

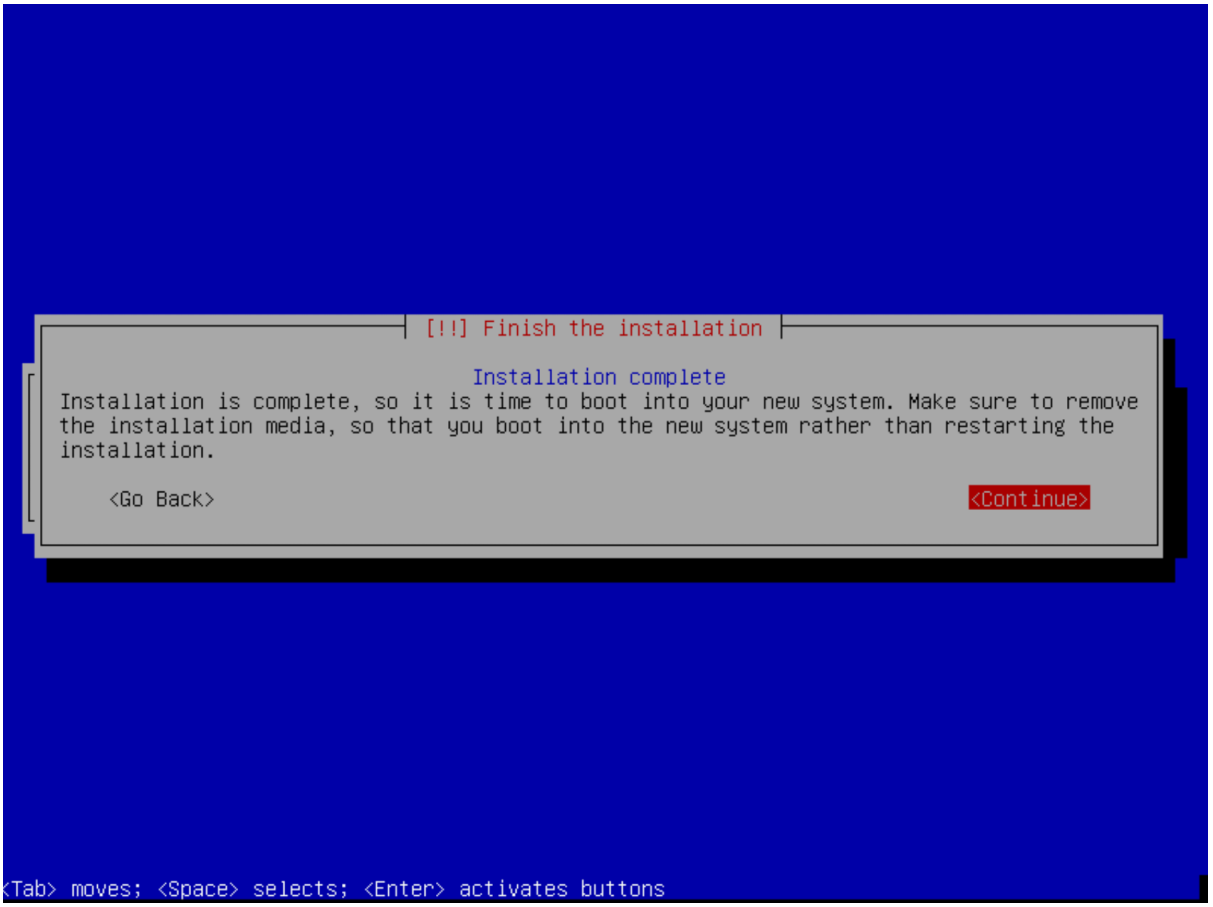


Install in the main partition the GRUB boot loader that will manage the system boot.





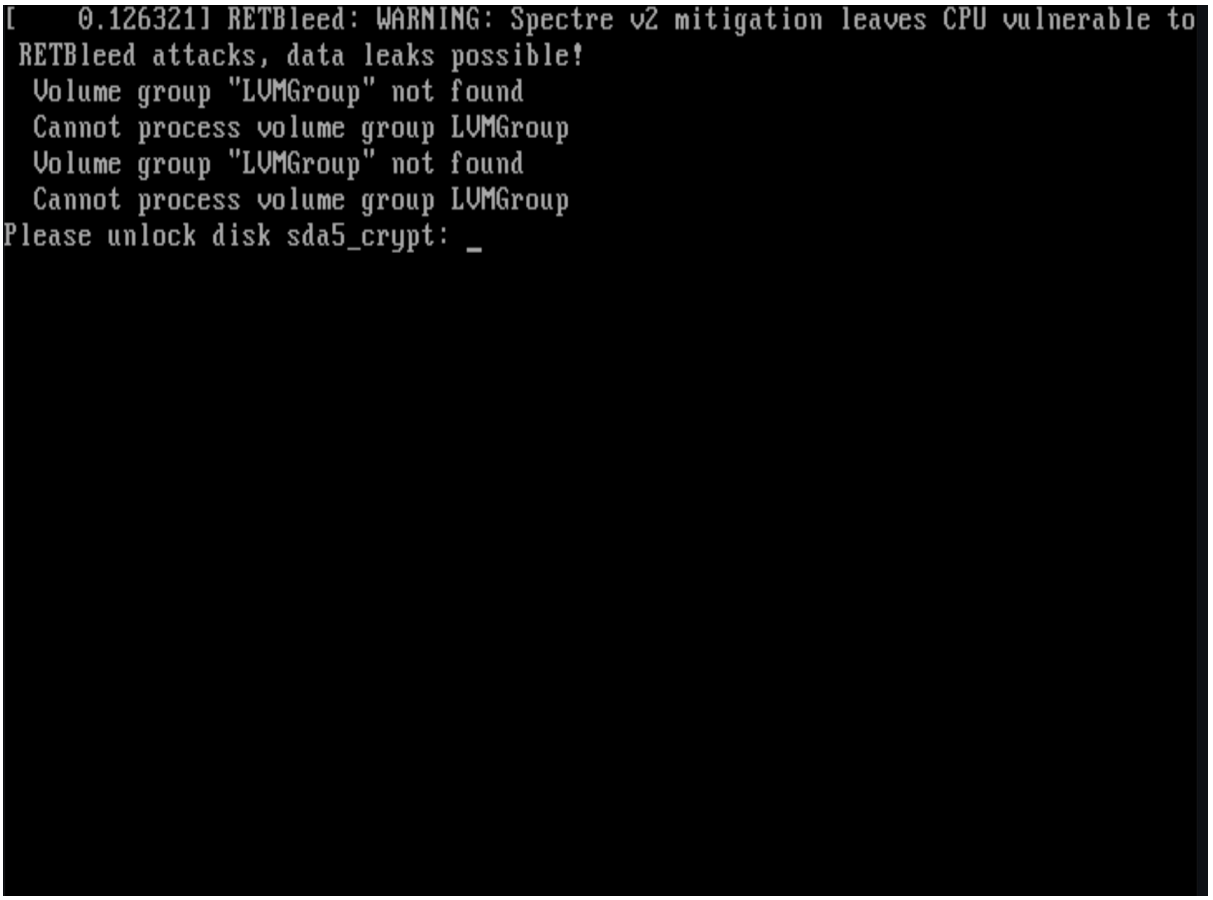
sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus



Installation completed. VBox should unmount the Debian iso. If not, do it manually like we did before when selecting the downloaded “.iso”.

2. Configuring the VM

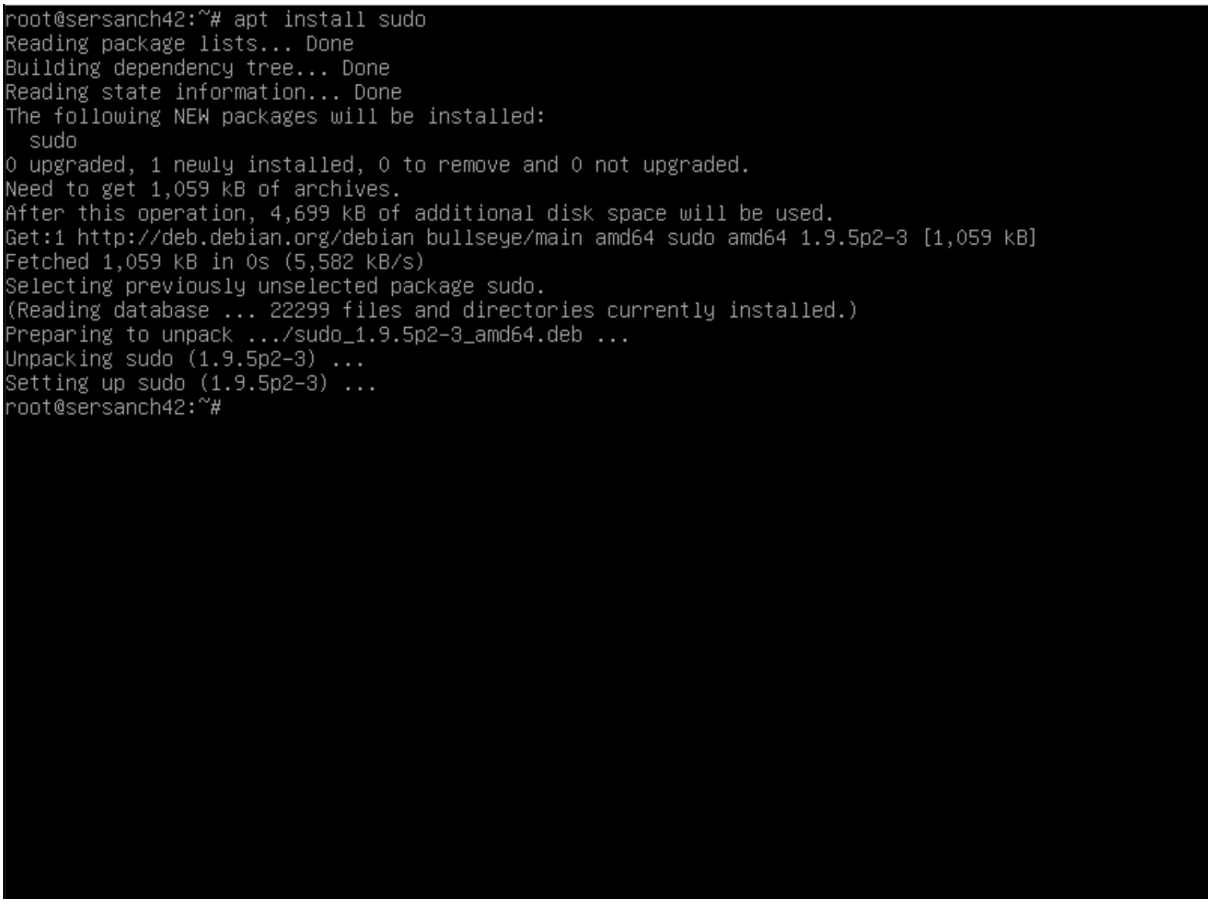
First use the password to decrypt the partitions.



Login as “root” and use the password you set before.

2.1 SUDO

Sudo is a command that allows a standard user to execute something with root privileges.
For installing, execute the following command:
apt install sudo
APT (**Advanced Packaging Tool**), allows us to manage and install software from repositories.



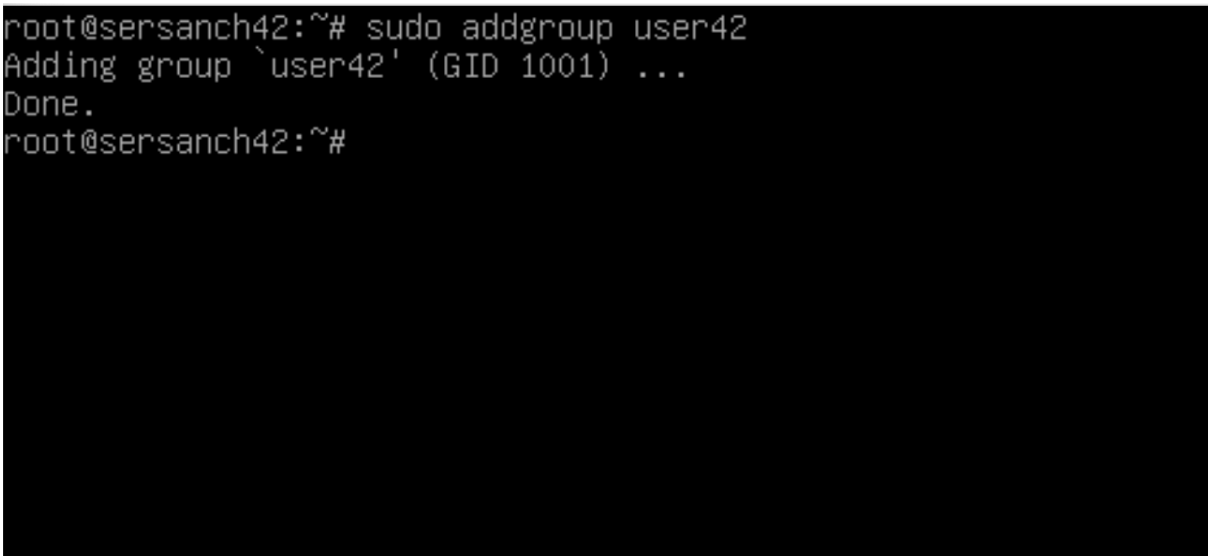
Reboot the system to apply the changes with:
sudo reboot

2.2 Add users

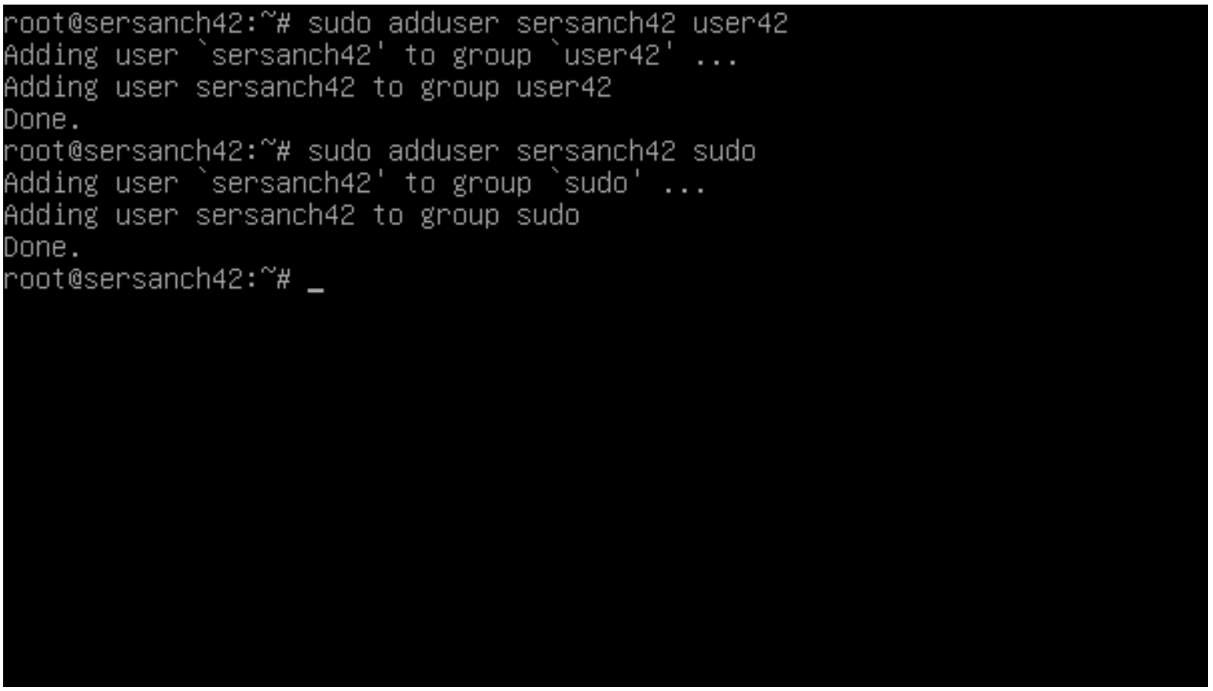
For adding users the command to use is
sudo adduser {login}
We have already added a standard user with my login so this section is for information only.
adduser command is a perl script that uses *useradd* command but is more user friendly.

2.3 Add groups

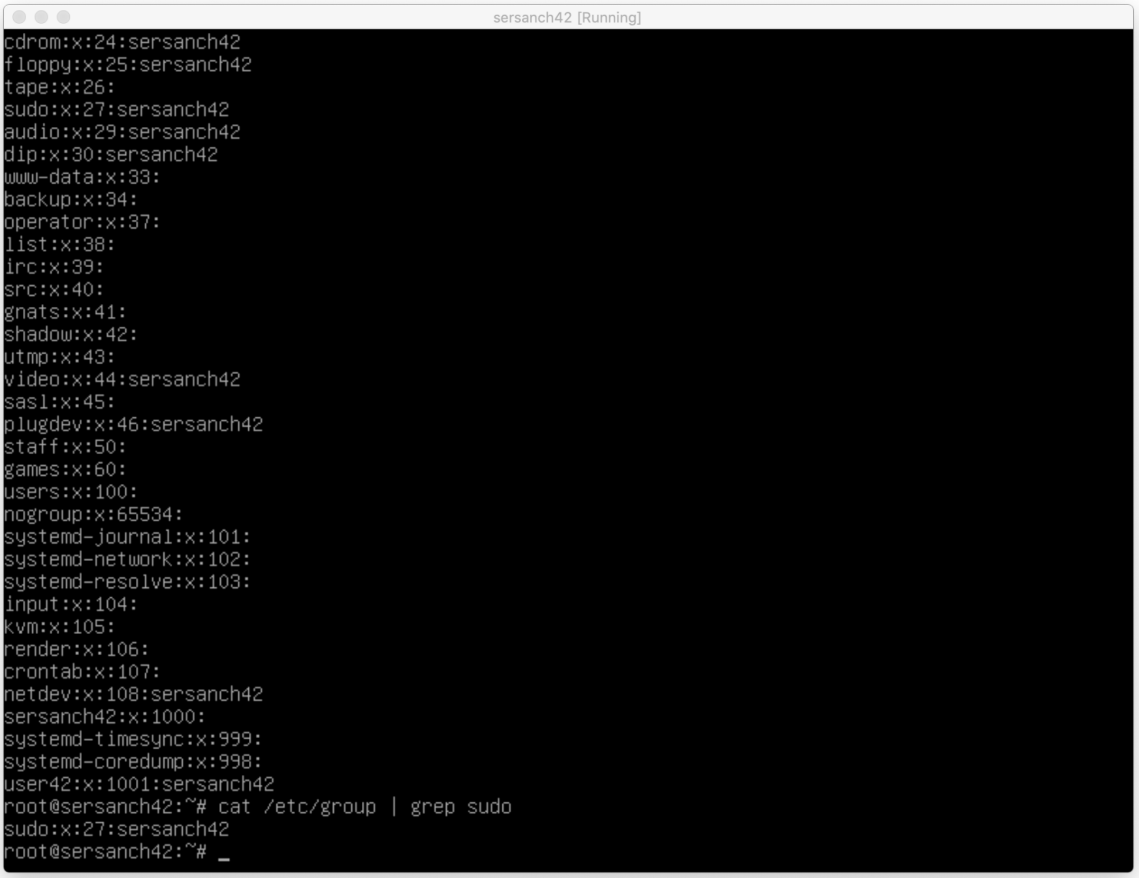
The subject is telling us to create a group called *user42.* The following command will create the group:
sudo addgroup {user}42



The group id (GID) is 1001.
Now, add the standard user to both sudo and user42 groups.

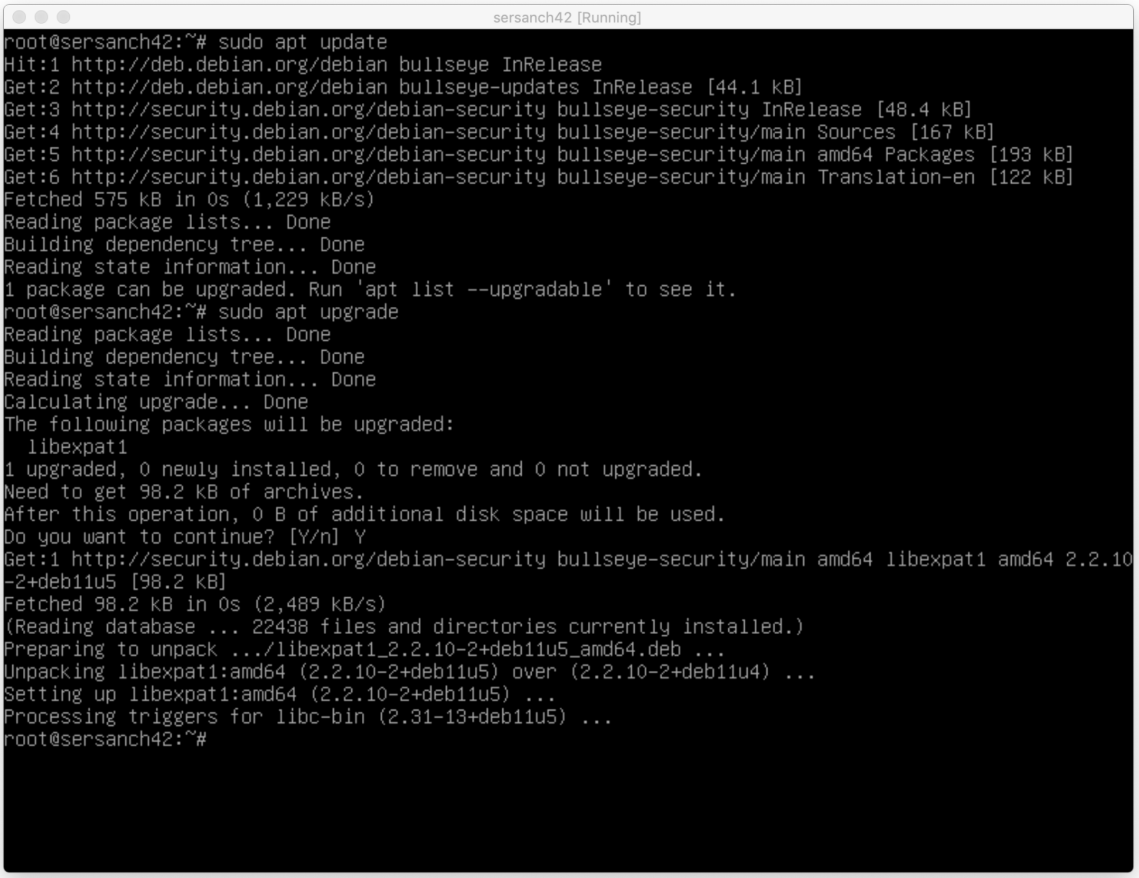


In /etc/group we can see the groups and its members.

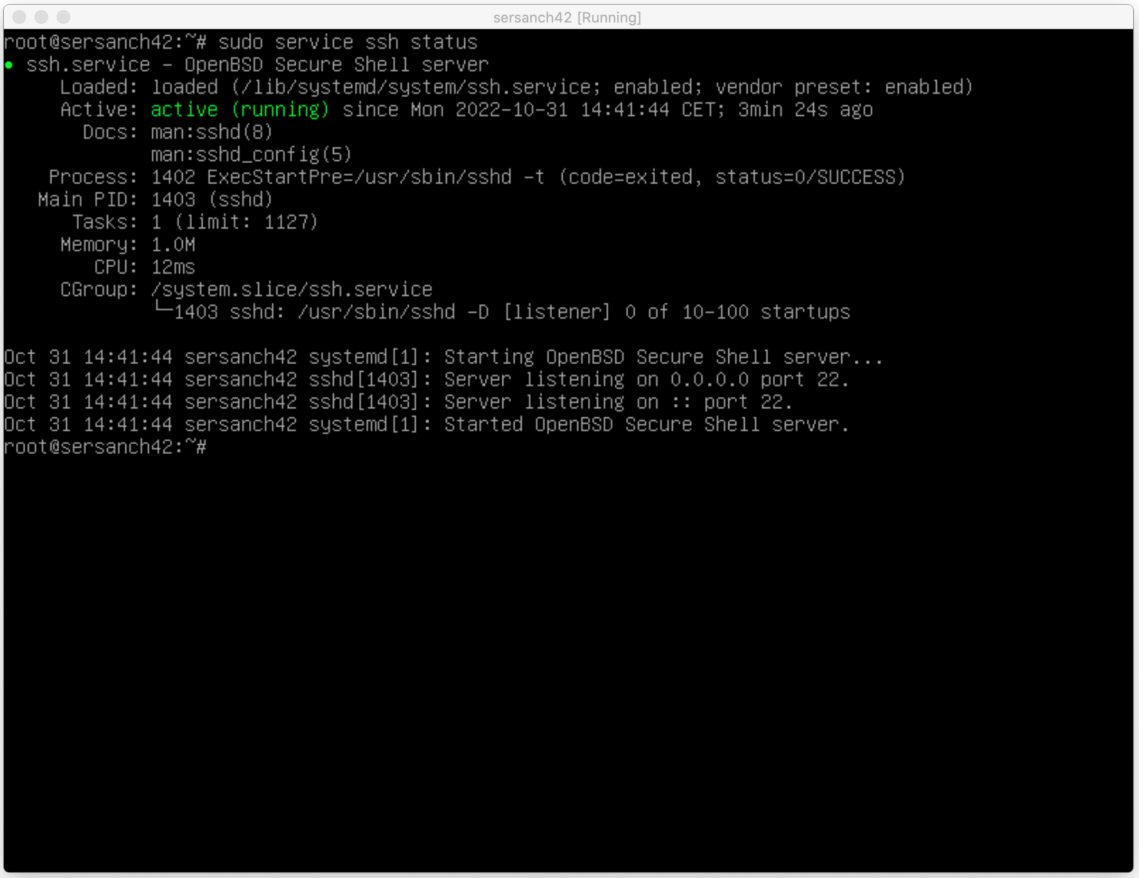


2.4 SSH

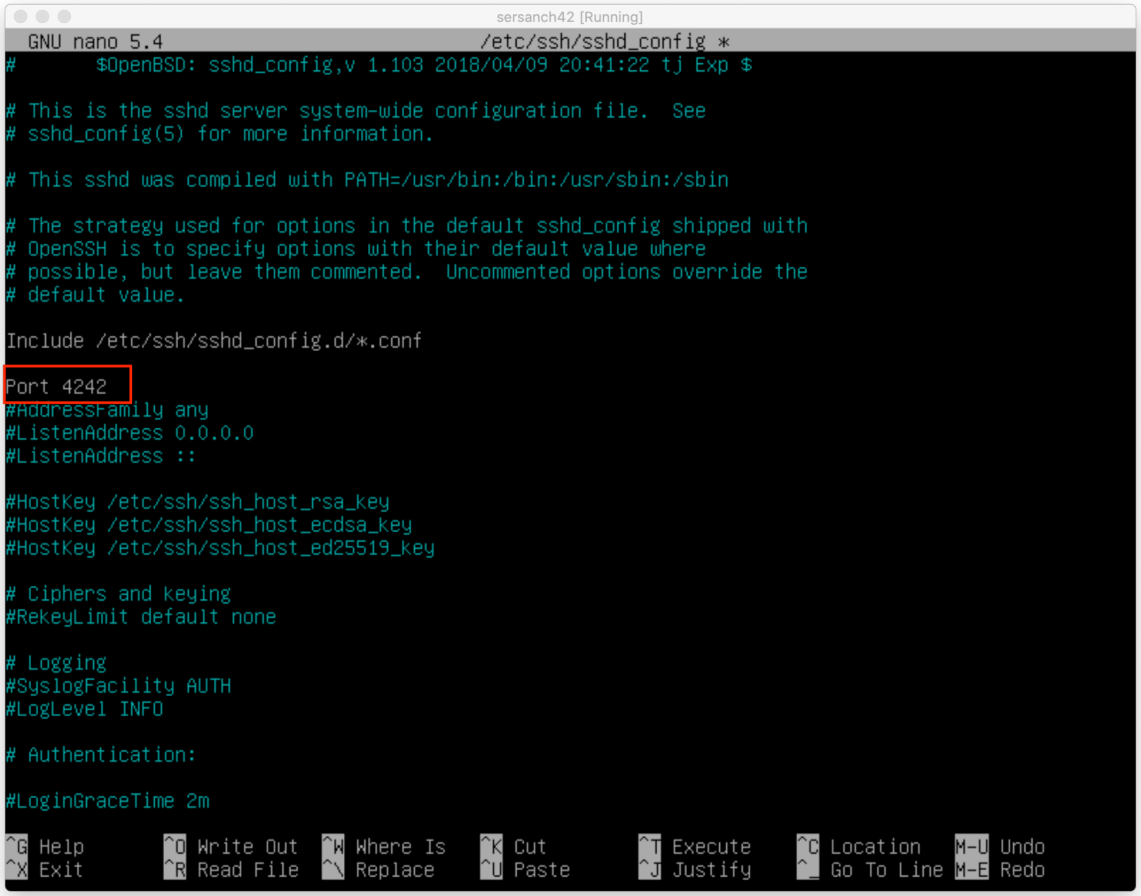
SSH is required to establish a connection to the server from remote access. It will be an encrypted, safe channel.
First, check that all packages are up to date and correctly installed using this two commands:
sudo apt update
sudo apt upgrade
Let's install it using the following command:
sudo apt install openssh-server



Once is installed, check if the process is running correctly using the following command: *sudo service ssh status*

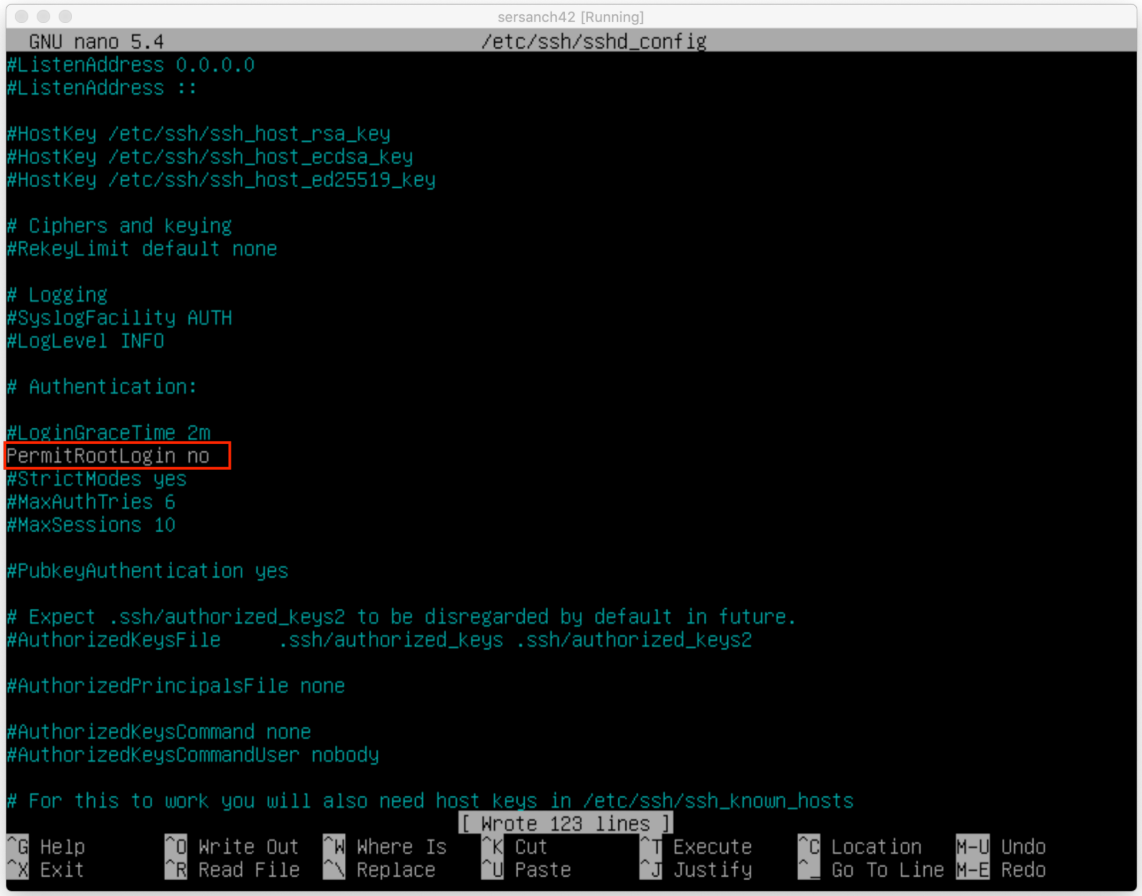


Now we need to configure some files (using sudo if needed).
First, open with *nano* command the file */etc/ssh/sshd_config*
Change the following lines, deleting the first “#” symbol for uncomment.
Port 22 → Port 4242
This will set the port of the ssh connection to 4242.

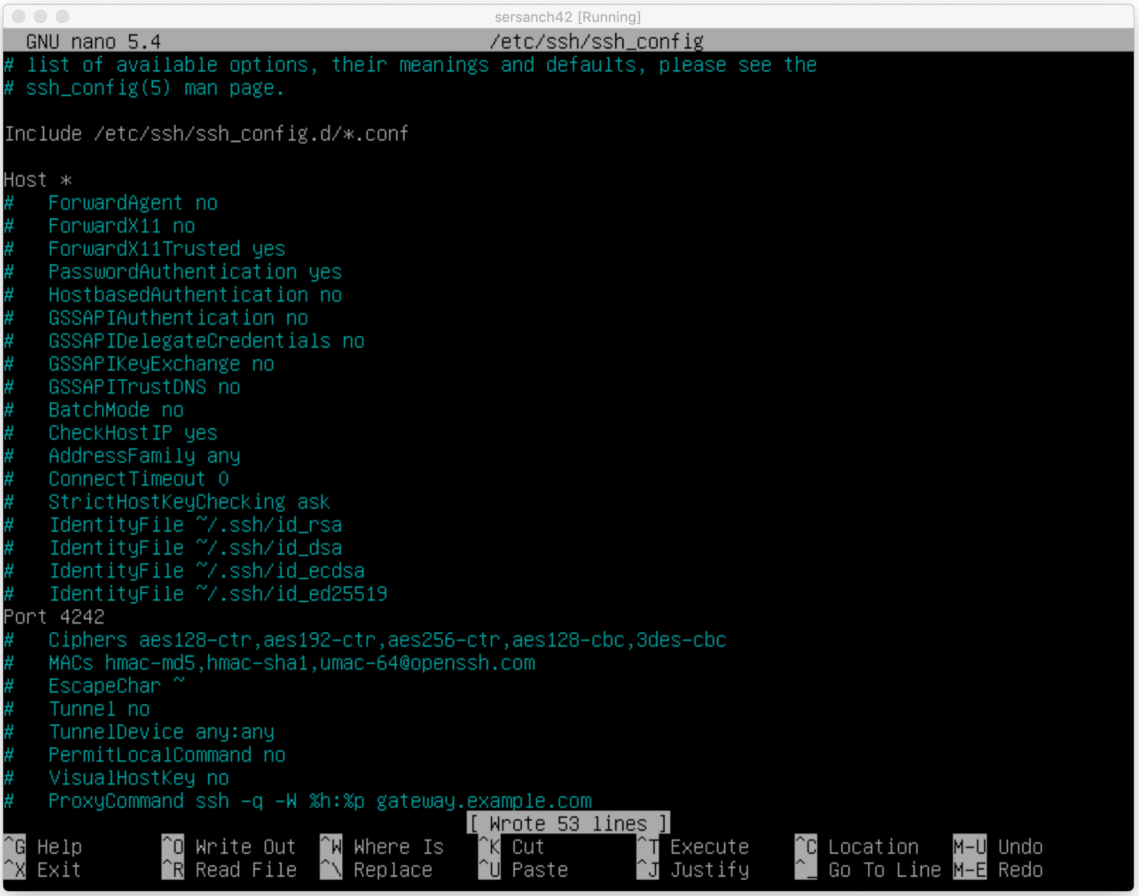


PermitRootLogin prohibit-password -> PermitRootLogin no
That will forbid root user connection with ssh.

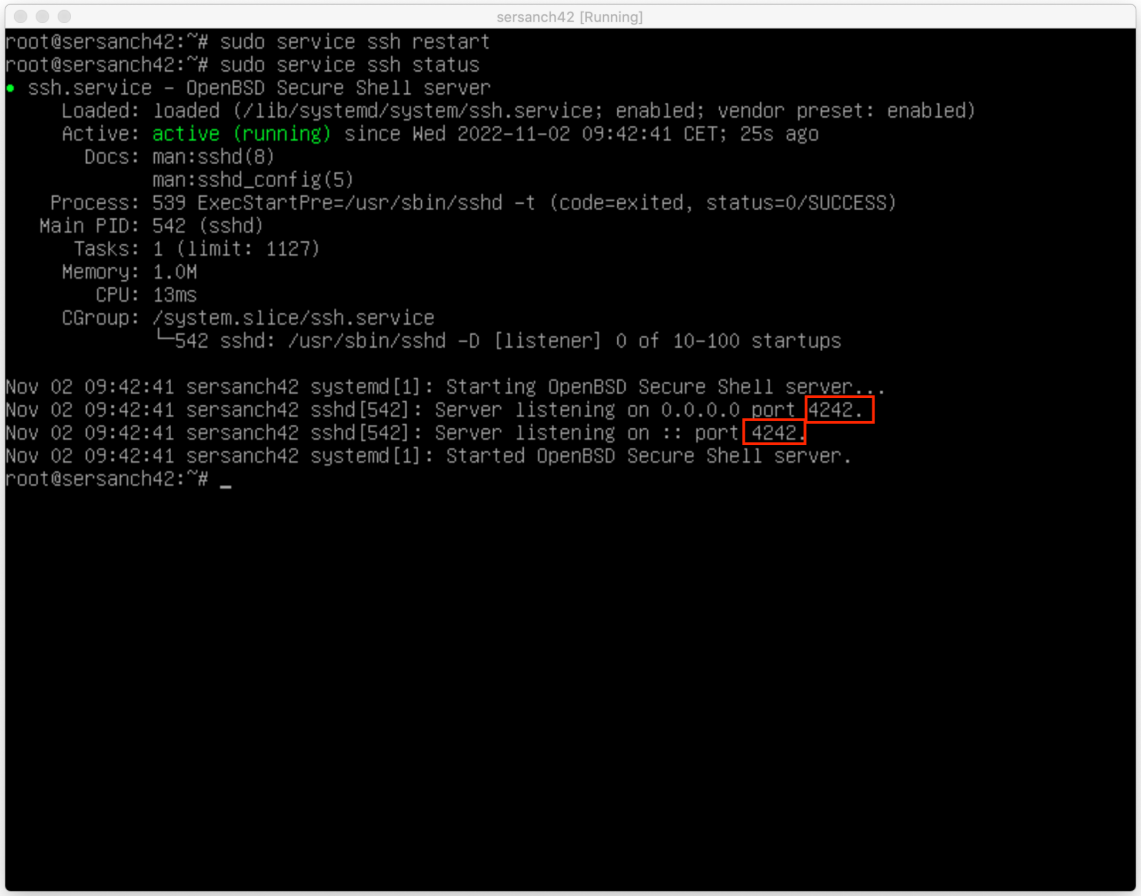
sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus



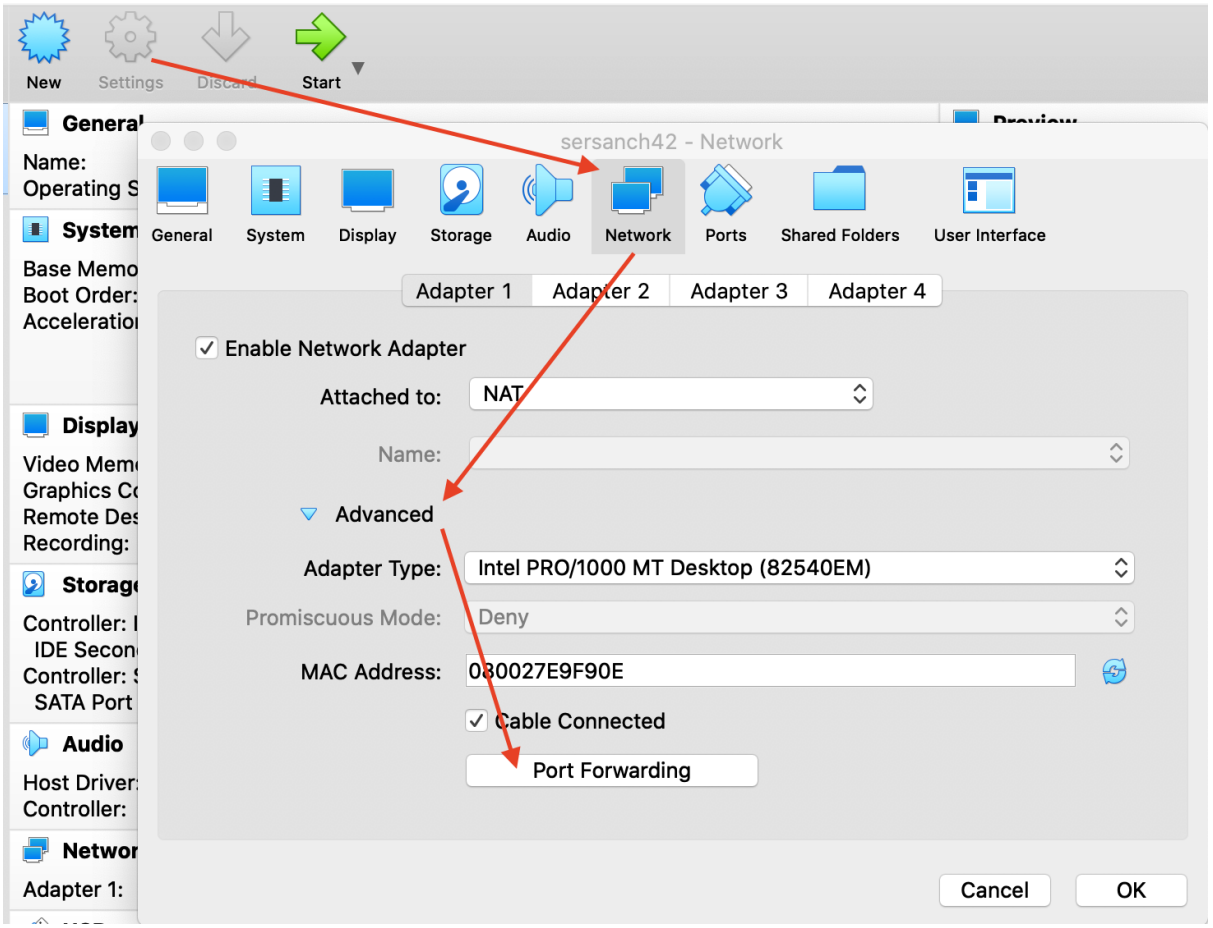
Save the file and close it.
Next, open */etc/ssh/ssh_config* file and update the port to 4242.



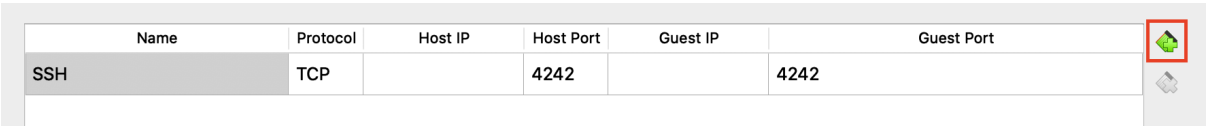
The last step is resetting ssh service. Use *sudo service ssh restart* to apply the changes made and check it with *sudo service ssh status.*



Power off the VM and go to VirtualBox settings → Network → Advanced → Port Forwarding

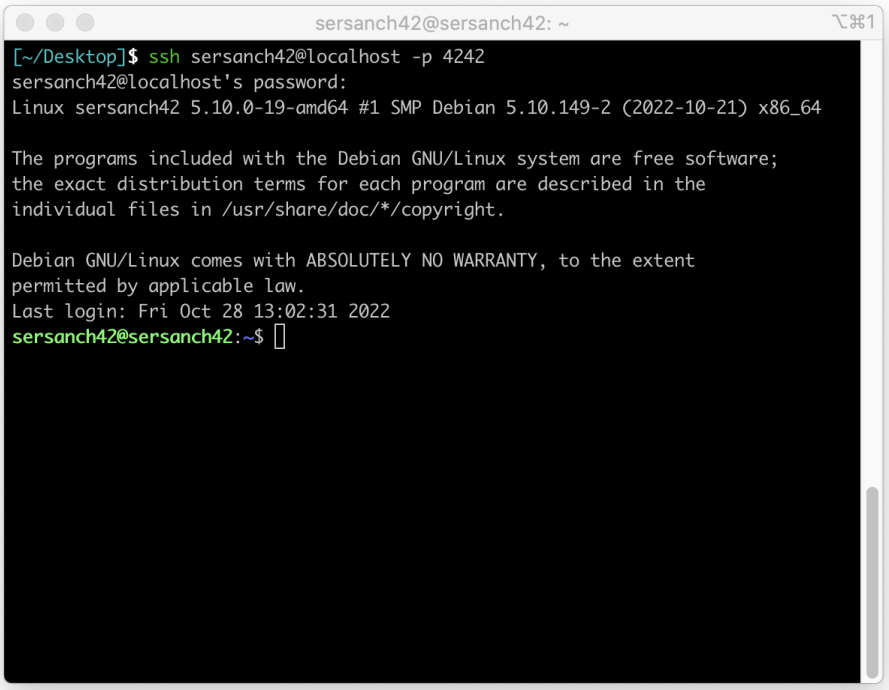


Add a new rule with TCP protocol and host/guest port = 4242 and click OK.



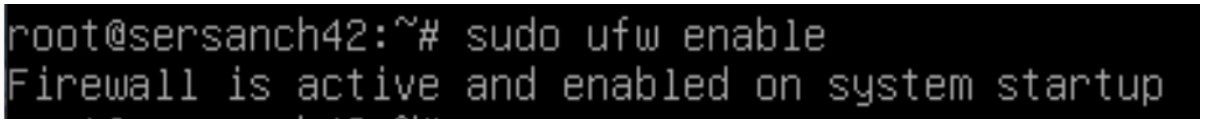
Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
SSH	TCP		4242		4242

From other PC with connection (or the host), open a terminal and write the following command using your username, but don't forget to turn on again the server:
ssh {username}@localhost -p 4242



2.5 UFW

UFW is a simple firewall that controls the network traffic using bash commands to configure the iptables.
First, for install UFW use the following command:
sudo apt install ufw
Following the UFW manual, let's enable it with:
sudo ufw enable



We will use port 4242 to establish the connections with SSH so we need to enable it.
sudo ufw allow 4242

```
root@sersanch42:~# sudo ufw allow 4242
Rule added
Rule added (v6)
root@sersanch42:~# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
4242                       ALLOW       Anywhere
4242 (v6)                  ALLOW       Anywhere (v6)
```

2.6 Strong password for SUDO

For configuring system rights, editing (or in our case, creating) a file in [*/etc/sudoers.d/*](/etc/sudoers.d/) is needed.
First create a file (choose the name you want) inside /etc/sudoers.d/ and open it with ***visudo***, for protecting the file against errors. The name of my file will be *sudo_config*.
Inside, we will write all the rules required by the subject.

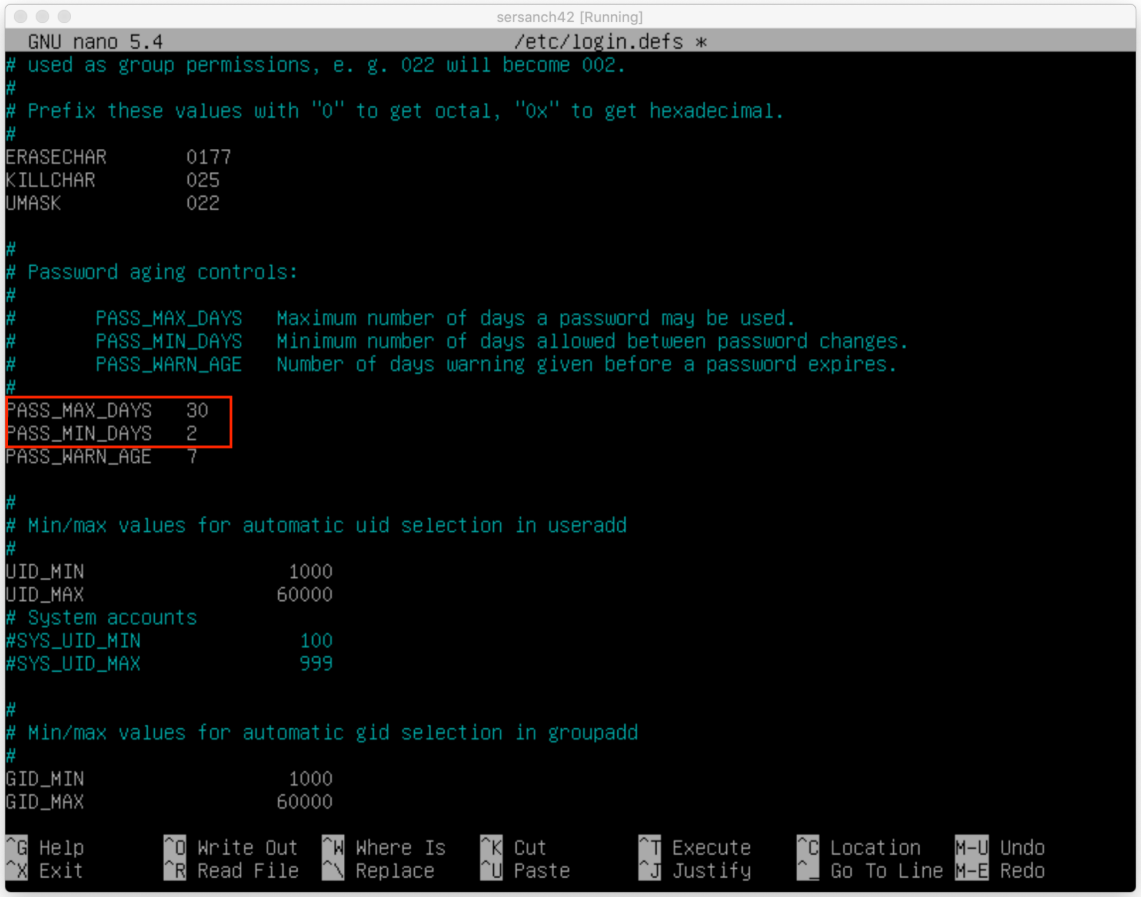
Defaults passwd_tries=3
Defaults badpass_message="Mensaje de error personalizado"
Defaults logfile="/var/log/sudo/sudo_config"
Defaults log_input, log_output
Defaults iolog_dir="/var/log/sudo"
Defaults requiretty
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

```
root@sersanch42:~# cat /etc/sudoers.d/sudo_config
Defaults        passwd_tries=3
Defaults        badpass_message="Incorrect SUDO password."
Defaults        logfile="/var/log/sudo/sudo_config"
Defaults        log_input, log_output
Defaults        iolog_dir="/var/log/sudo"
Defaults        requiretty
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
```

passwd_tries=3 → Max password tries.
badpass_message= → Message that will be shown when incorrect password is used.
logfile= → Path where log of sudo commands will be stored.
log_input, log_output → Stores the input and output of the sudo commands executed.
iolog_dir= → Path where the input and output sudo commands will be stored.
requiretty → TTY is mandatory to run sudo commands. That means that you need to be logged in to execute sudo commands. For example, a crontab won't be able to.
secure_path → Paths (in order) where the sudo execution will try to find the specified command.

2.7 Strong password policy

The password policy is specified in the file */etc/login.defs* . Inside, we will use the options that are required by the subject.
Edit */etc/login.defs* file and modify the following parameters.



PASS_MAX_DAYS → Days until your password expires.

PASS_MIN_DAYS → Min days to pass before changing the password again.

PASS_WARN_AGE → Days left where a warning message for change the password is sended to the user.

Now, we need to install libpam-pwquality with the following command. That program checks if the password is similar to others or has patterns that are not allowed.
sudo apt install libpam-pwquality
Let's edit the config file in /etc/pam.d/common-password and put, after "retry=3" all the following rules:
minlen=10
ucredit=-1
dcredit=-1
maxrepeat=3
reject_username
difok=7

sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus

enforce_for_root

```
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3 minlen=10 ucredit=-1 dcred>
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yesc>
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
```

minlen=10 → Min password length.
ucredit=-1 → Min 1 uppercase letter. (+ for max if required)
dcredit=-1 → Min 1 digit
maxrepeat=3 → Max repeated characters in a row.
reject_username → Forbid username inside the password.
difok=7 → Min number of characters different to the last password.
enforce_for_root → Ensure that these options will be applied to root too.

2.8 Information script

The subject tells us to build a script to show some info about our system. We are going to explain it line by line. The variable names could be others.

“The architecture of your operating system and its kernel version.”
uname -a
Prints all the operating system info.
For executing a command inside a bash script, use $({command})

“The number of physical processors.”
For the processors we will see the content of */proc/cpuin*
This file displays each processor info so we will count the number of lines inside for get the amount of processors.
grep “physical id” /proc/cpuinfo | wc -l

“The number of virtual processors.”
grep “processor” /proc/cpuinfo | wc -l

“The current available RAM on your server and its utilization rate as a percentage.”
This part is going to be split into different things.
Used RAM → *free --mega | grep "Mem" | tr -s ' ' | cut -d " " -f3*
Total RAM → *free --mega | grep “Mem” | tr -s ‘ ‘ | cut -d “ “ -f2*

“The current available memory on your server and its utilization rate as a percentage.”
Same as the RAM. We will find the info using the command *df* (disk free).
We need to delete from calculation “tmpfs” (temporary file system for keeping things in virtual memory) and “udev” (info about plugged in devices). Also “/dev/loop” if it exists, but we don’t have it. Then, sum all available and used space with *awk* command.
Used memo → *df -m | egrep -v "udev|tmpfs|Filesystem" | awk '{used_memo+=$3} END {print used_memo}'*
Total memo → *df -m | egrep -v "udev|tmpfs|Filesystem" | awk '{used_memo+=$2} END {print used_memo}'*
Note: the -m flag is the same as -Bm, that is used to indicate that the result will be in MB.

“The current utilization rate of your processors as a percentage.”
top command tells us the percentage of CPU(s) active. If we subtract 100 to the idle percentage, we will get the active usage. The problem is that *top* command doesn’t stop when it is executed so we need to use flags to ensure one batch of info only and do the operation with the idle percentage and print it with two decimals.
top -b -n 1 | grep "%Cpu(s)" | awk -F',' '{calc=100-$4} END {printf "%.2f%%", calc}'

“The date and time of the last reboot.”
who -b
This command displays info about the last reboot but the format could vary using different localization. So, we are going to select the info after “system boot”.
who -b | tr -s ‘ ‘ | cut -d’ ‘ -f4-
-fX- is used to select all the columns after X. In our case, 4 is the column where the date starts.

“Whether LVM is active or not.”
In the “*/etc/fstab*” file we find all the partitions in the system. We need to find if there is any “lvm” in type. These type of partitions are described by /dev/mapper/*.
cat /etc/fstab | grep “^/dev/mapper/” | wc -l
Now that we have counted the lvm partitions, we need to do a conditional to choose the correct output.

```
lvm_active=$(cat /etc/fstab | grep "^/dev/mapper/" | wc -l)
if [[ $lvm_active -gt 0 ]]
then
        lvm_active="yes"
else
        lvm_active="no"
fi
```

“The number of active connections.”
With *ss* command we can see all (-a flag) the active connections. We need to count the ones with the established status using TCP protocol (-t flag).
ss -ta | grep “ESTAB” | wc -l

“The number of users using the server.”
users | wc -w

“The IPv4 address of your server and its MAC (Media Access Control) address.”
IPv4 → *hostname -I*
For the MAC address we need to find the main interface with “link/ether”
MAC → *ip link | grep "link/ether" | tr -s ' ' |cut -d' ' -f3*

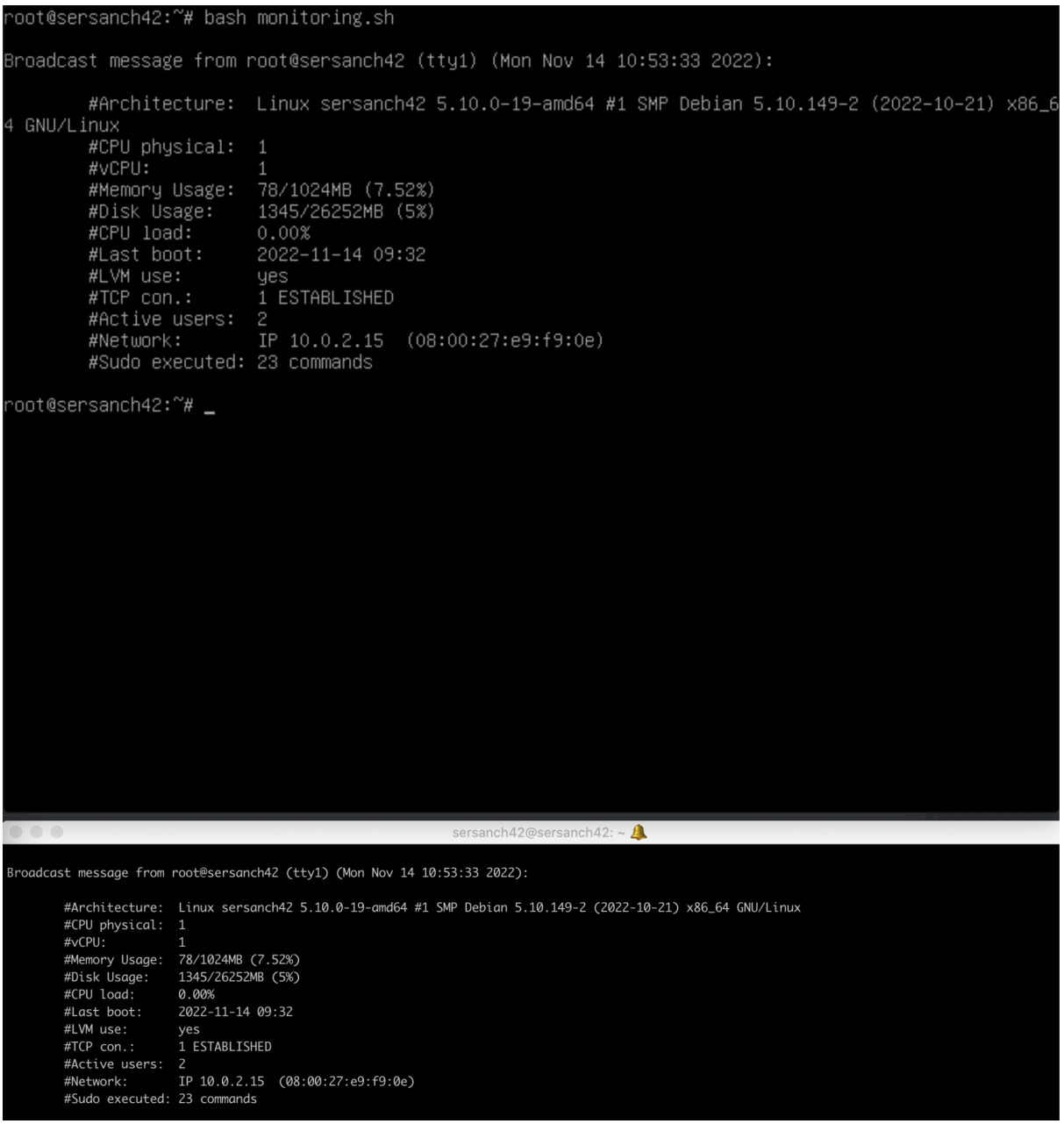
“The number of commands executed with the sudo program.”
The sudo commands are registered in */var/log/sudo/sudo_config* file. We need to filter the lines and count them.
cat /var/log/sudo/sudo_config | grep “COMMAND” | wc -l
Note that “sudo_config” is a custom name I chose before.

Now that we have all the variables, let’s print it with some pretty stuff. But for now, get the percentage of RAM and disk usage using:
RAM → *free --mega | awk '$1 == "Mem:" {printf("(%.2f%%)\n", $3/$2*100)}'*
Disk → *df -m | egrep -v "udev|tmpfs|Filesystem" | awk '{disk_used += $3} {disk_total += $2} END {printf("%d", disk_used/disk_total*100)}'*

This is the final view of the code.

Finally execute it to see if it works properly.

sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus



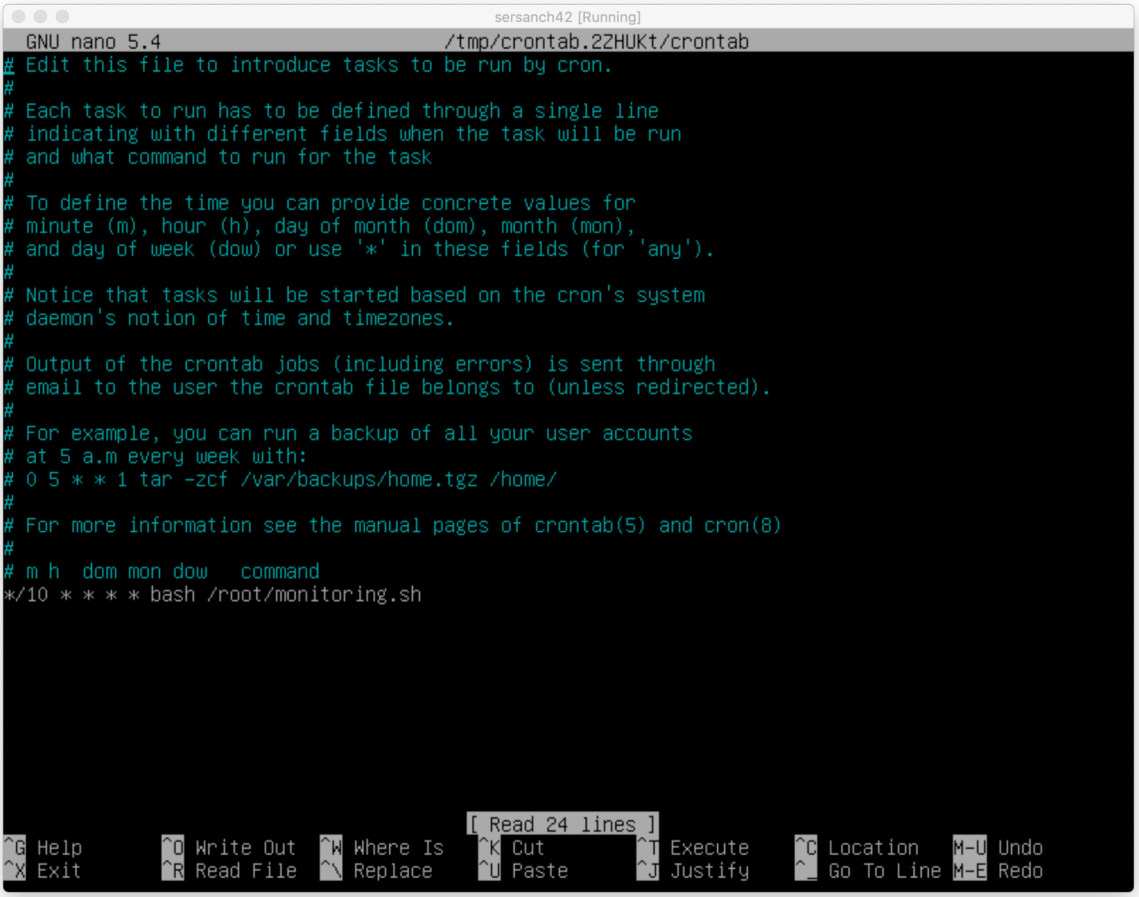
The subject indicates that we need to execute this script every 10 minutes. Crontab will be the solution.

2.9 Crontab

Crontab is a file used to specify different configurations for executing daemons (background processes).
We could simply edit directly */etc/crontab* file, but if we make any errors, the other daemons will not be executed. So first, we need to use *crontab -e -u root* command that makes a copy of crontab into /tmp. With -u flag, we will be sure that it will be edited by root user.

crontab -e -u root

Select the editor you want to use. I will use nano.
The syntax to configure crontab is as follows:
m h dom mon dow user command
m = minute
h = hour
dom = day of month
mon = month
dow = day of week
user = linux user that will run the command (only in crontab file)
command = the linux command that needs to be run.



“*/10” means execute every 10min.
If you need to see the script is saved in the following path:
/var/spool/cron/crontabs/{user}

3. Bonus

3.1 Wordpress

3.1.1 lighttpd

lighttpd is a fast web server perfectly made for our light server.
It will be using the HTTP port (80).
sudo apt install lighttpd
As we did before, configure the firewall to allow port 80 connections.
sudo ufw allow 80
Check the status with
sudo ufw status

```
root@sersanch42:~# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
4242                       ALLOW       Anywhere
80                         ALLOW       Anywhere
4242 (v6)                  ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
```

3.1.2 MariaDB

MariaDB is an open source database based on MySQL.
sudo apt install mariadb-server
For configuring its security, execute the following command:
sudo mysql_secure_installation
A lot of questions for configured MariaDB will be asked. Answer YES to all except for “Switch to unix-socket authentication” and “Change the root password”, because our admin is already configured.
Now, open MariaDB terminal with *sudo mariadb* and create a new database. I’ve chosen “bonus” name. Reference link.
CREATE DATABASE bonus;
Use *SHOW DATABASES;* to check if it is correctly created.

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| bonus              |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.000 sec)
```

The next step is optional but I will create a new user in MariaDB that will have all privileges on the “bonus” table.

CREATE USER 'admin'@localhost IDENTIFIED BY 'Password42'

Grant access to new user with:
GRANT ALL PRIVILEGES ON bonus. TO 'admin'@localhost IDENTIFIED BY 'Password42';*
MySQL refreshes automatically the grants and privileges. If not, use the following command:
FLUSH PRIVILEGES;

3.1.3 PHP

sudo apt install php-cgi php-mysql
php-cgi → Bridge between user interface and DB.
php-mysql → Software that is used to connect with MySQL.
Check if is correctly installed with → php --version

3.1.4 WordPress

https://github.com/GuillaumeOz/Born2beroot
First, install wget. wget is used to retrieve content from a web server, like files for example.
sudo apt install wget

Download Wordpress from official web:
sudo wget http://wordpress.org/latest.tar.gz -P /var/www/html
We are saving it in /var/www/html because in this directory is where the web server will have the files by default. "-P" flag is for specifying the directory to save the files.

Extract the downloaded files with:
sudo tar -xzvf /var/www/html/latest.tar.gz
-x → extract
-z → because is compressed
-v → Optional verbose.
-f → Specify the file to extract.
And remove the compressed file no longer needed:
sudo rm /var/www/html/latest.tar.gz
Copy the content in wordpress folder into the root web service folder and delete the original folder:
sudo cp -r {your path where wordpress is}/wordpress/ /var/www/html*
sudo rm -rf {your path where wordpress is}/wordpress

```
root@sersanch42:~# ls /var/www/html
index.lighttpd.html  wp-admin             wp-cron.php        wp-mail.php
index.php            wp-blog-header.php   wp-includes        wp-settings.php
license.txt          wp-comments-post.php wp-links-opml.php  wp-signup.php
readme.html          wp-config-sample.php wp-load.php        wp-trackback.php
wp-activate.php      wp-content           wp-login.php       xmlrpc.php
root@sersanch42:~#
```

The next step is to make a configuration file for WordPress, using the example:
sudo cp /var/www/html/wp-config-sample.php /var/www/html/wp-config.php

Open *wp-config.php* with nano and let's configure it for using WordPress with MariaDB created before. Replace the content with the correct names of database, user, and password:
line23 define('DB_NAME', 'bonus');
line26 define('DB_USER', 'admin');
line29 define('DB_PASSWORD', 'Password42');

```
** Database settings - You can get this info from your web host ** //
* The name of the database for WordPress */
efine( 'DB_NAME', 'bonus' );

* Database username */
efine( 'DB_USER', 'admin' );

* Database password */
efine( 'DB_PASSWORD', 'Password42' );

* Database hostname */
efine( 'DB_HOST', 'localhost' );

* Database charset to use in creating database tables. */
efine( 'DB_CHARSET', 'utf8' );

* The database collate type. Don't change this if in doubt. */
efine( 'DB_COLLATE', '' );
```

3.1.5 Finishing WordPress installation

Finally, we need to enable some modules of lighttpd:
sudo lighty-enable-mod fastcgi
sudo lighty-enable-mod fastcgi-php
Fastcgi is like cgi but it allows the web server to manage more connections at the same time.

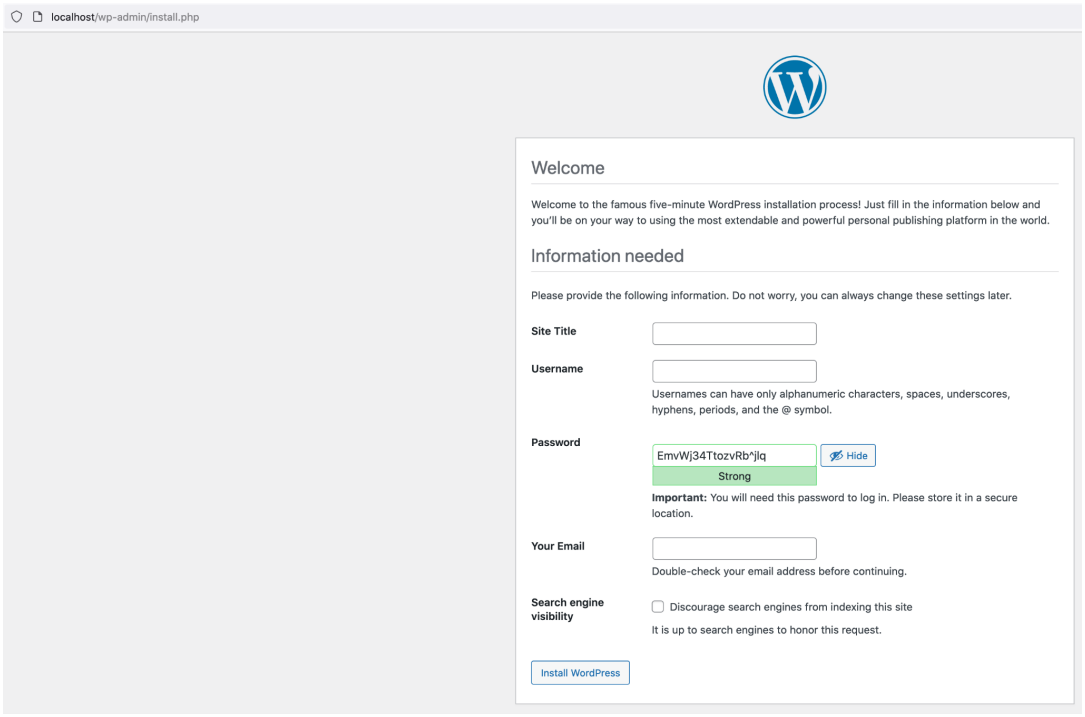
And restart the service:
sudo service lighttpd force-reload

Check that the services are active and working:
sudo systemctl status lighttpd.service
sudo systemctl status mariadb

Finally, don't forget to open port 80 in VirtualBox configuration in *Settings → Network → Advanced → Port Forwarding*

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
HTTP	TCP		80		80
SSH	TCP		4242		4242

Go to http://localhost/wp-admin/install.php and you should see the following page. WordPress is correctly installed and running.



3.2 FTP service

FTP (file transfer protocol) is used to communicate and transfer files between different computers, using TCP/IP protocol and secure it with users and permissions.
We will be using vsftpd, so let's install it and ftp server.
sudo apt install vsftpd
sudo apt install ftp

Open the port 21, which is used for FTP:
sudo ufw allow 21

Edit fsftpd config file in "/etc/vsftpd.conf". To enable any write command, uncomment the following line:
write_enable=YES

We don't want the user to be roaming outside the default directory tree so, uncomment this:
chroot_local_user=YES

Specify the user and folder adding this at top of the file:
user_sub_token=$USER
local_root=/home/$USER/ftp

Now, let's create a folder for my user to store the files and assign the privileges. Basically, delete all groups from this folder and delete write permissions to anybody except root and the owner:

sudo mkdir /home/sersanch42/ftp
sudo chown nobody:nogroup /home/sersanch42/ftp
sudo chmod a-w /home/sersanch42/ftp

Create “/etc/vsftpd.userlist” file and add inside the username, sersanch42 and add these lines:
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO

Finally, don’t forget to open port 21 in VirtualBox configuration in *Settings → Network → Advanced → Port Forwarding*

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
HTTP	TCP		80		80
SSH	TCP		4242		4242
FTP	TCP		21		21

Finally check the status of FTP service:
sudo systemctl status vsftpd.service

4. Asked questions in the evaluation

4.1 How a virtual machine works

A VM is a software that emulates the hardware (virtualization) and has its own software for executing processes and applications.

4.2 Why did you choose this OS?

Easy to configure, install and keep up to date.

4.3 Differences between CentOS and Debian

Source1 Source2	Debian	CentOS
File System	EXT4	XFS
Package format	DEB format -> dpkg/APT (packet manager)	RPM format-> YUM/DNF (packet manager)
Architecture	Less quantity	More quantity
Support	A lot of community support and Red Hat Limited	Least support

Updates	Long time without big changes. Updating is tedious.	Regular updates and easy to do the transition.
Interface	More difficult to use	Easy to use and friendly interface

4.4 The purpose of virtual machines

Using a virtual machine allows us to have different SO inside one PC with the advantage that it is fully isolated from one to another. It lets us try different programs without the fear of having an “explosion” on our real PC if we mess with something. Also, having snapshots makes the recovery process faster. It’s easier to administer because the VM could be duplicated or simply import the VM file into another PC and you will have the same configuration.

4.5 Difference between aptitude and apt

Aptitude is an user-friendly interface for getting packages with apt, the advanced package manager. Aptitude lets us do advanced search and manages the dependencies easily.

4.6 What is AppArmor

AppArmor is a program that restricts the actions processes can take, increasing the security in the system, specially in the software with more vulnerabilities.

5. Summary

Check UFW
systemctl status ufw
sudo ufw status
Delete rule → *ufw status numbered* → *ufw delete {rule num}*
Check SSH
systemctl status ssh
Connect with ssh from another connection:
ssh {user}@localhost -p 4242
Check SO
uname -a

Check that user is added to sudo and its own user groups
groups sersanch
Create an user
sudo adduser {users}
How password policy was set
link
/etc/sudoers.d/sudo_config

sszahinos - https://github.com/sszahinos/born2beroot
42Barcelona cursus

Create group and assign the created user
addgroup {group name}
adduser {user} {group}

Check hostname
hostname
Replace hostname
hostname {name}
nano /etc/hostname
nano /etc/hosts and replace old with new.
hostnamectl set-hostname {nombre host}
Show partitions
lsblk
What is LVM
LVM is Logical Volume Management, a more advanced and flexible system than the traditional partitioning disks into different segments.
With LVM we can make a group of different physical volumes and separate it into different logical volumes, equivalent to partitions.

Check sudo
/bin | grep "sudo"
sudo -V
/var/log/sudo

What is cron
Crontab is a file used to specify different configurations for executing daemons (background processes).
systemctl stop cron
Check */var/spool/cron/crontabs/*

PHP
php -v

FTP
systemctl status vsftpd.service

lighttpd
systemctl status lighttpd

Cron
service cron stop