FUSS - Handbook for the technician

Release 12.0

FUSS Lab

Jul 14, 2023

Index

1 Quick installation guide **3**
1.1 Topology of a typical educational network 3
1.2 Installation of FUSS server from the cloud-init ready template....4
1.3 Installation of traditional FUSS server 8
1.4 Traditional installation of FUSS Client....33
1.5 Installation with FUSS-FUCC 60
1.6 Captive Portal/WiFi Network Management....62

2 Architecture **65**
2.1 Services present on Fuss Server 65

3 FUSS server management **67**
3.1 Server configuration....67
3.2 Server access....68
3.3 The main configuration files....68
3.4 Updates 71
3.5 Backup with fuss-backup....73
3.6 Home Cleaning 75
3.7 Netmask modifications 76
3.8 Troubleshooting - Troubleshooting....76

4 FUSS client management **83**
4.1 Configuring a *FUSS Client*....83
4.2 Updates 85
4.3 Key access to fuss-client server....85
4.4 Troubleshooting 87
4.5 Alternative procedures....87

5 The OctoNet management interface **91**
5.1 Architecture 91
5.2 Managing Users and Groups 94
5.3 Host management 123
5.4 Web filter management....135
5.5 Firewall management....141
5.6 Network Printers 148
5.7 Share Samba 159

6 Classroom management **167**
6.1 Foreword....167
6.2 The script....167
6.3 The csv files....169

6.4 Conclusions 170

7 Fuss Manager **171**

8 Specialized installations **173**
8.1 Installing Debian on Software RAID 173
8.2 Installing Proxmox on Debian 205
8.3 Direct installation of Proxmox 212
8.4 Installation of fuss-server on Proxmox 214
8.5 Machine cloning with clonezilla 233
8.6 Installations in schools in the Autonomous Province of Bolzano. 260

9 Bug reporting **267**
9.1 Information gathering 267

10 Policies **269**
10.1 Authentication specifications 269
10.2 Internet access 270

11 Dump and restore **273**
11.1 Update fuss-server via dump and restore 273
11.2 Dumping operations on the original server (FUSS8) 273
11.3 Operations on the new server (FUSS10) 273

12 Hardware miniguides **275**
12.1 PC with special requirements 275
12.2 Notebooks with special requirements 276
12.3 Management and installation of printers and scanners 285
12.4 Reader for health card or CNS/CPS 297
12.5 Installation of electronic ID card reader 298
12.6 Change the disk type of the FUSS Server 300
12.7 UPS 302
12.8 Interactive whiteboards and video projectors 305

13 Miniguide software **311**
13.1 Configuring fuss-server to enable mail sending 311
13.2 Problems with CDs and DVDs 312
13.3 Chromium settings 314
13.4 Installation of the iprase game package 316
13.5 Share Samba with subfolder structure 317
13.6 Updating fuss-clients via fuss-cru 318
13.7 Configuration for the use of OCS inventory agent 318

14 Idea Incubator **321**
14.1 Proposal 1: Installation of FUSS Server starting from Debian Cloud upstream 321
14.2 Proposal 2: Soft migration from FUSS 8 server to FUSS 10 server. 322

15 Contribute **327**
15.1 Authors 327

16 Support **329**

17 Licenses **331**

This manual is a guide aimed at FUSS technicians for maintaining a FUSS GNU/Linux installation based on Debian 12 "Bookworm."

The most recent version of this manual can be read at https://fuss-tech-guide.readthedocs.io/en/latest/



CHAPTER 1

This chapter is for those who want to quickly see how to install a FUSS server and client.

1.1 Topology of a typical network teaching

Before showing how to install servers and clients, let us see in the following figure the typical network topology where FUSS can find application.

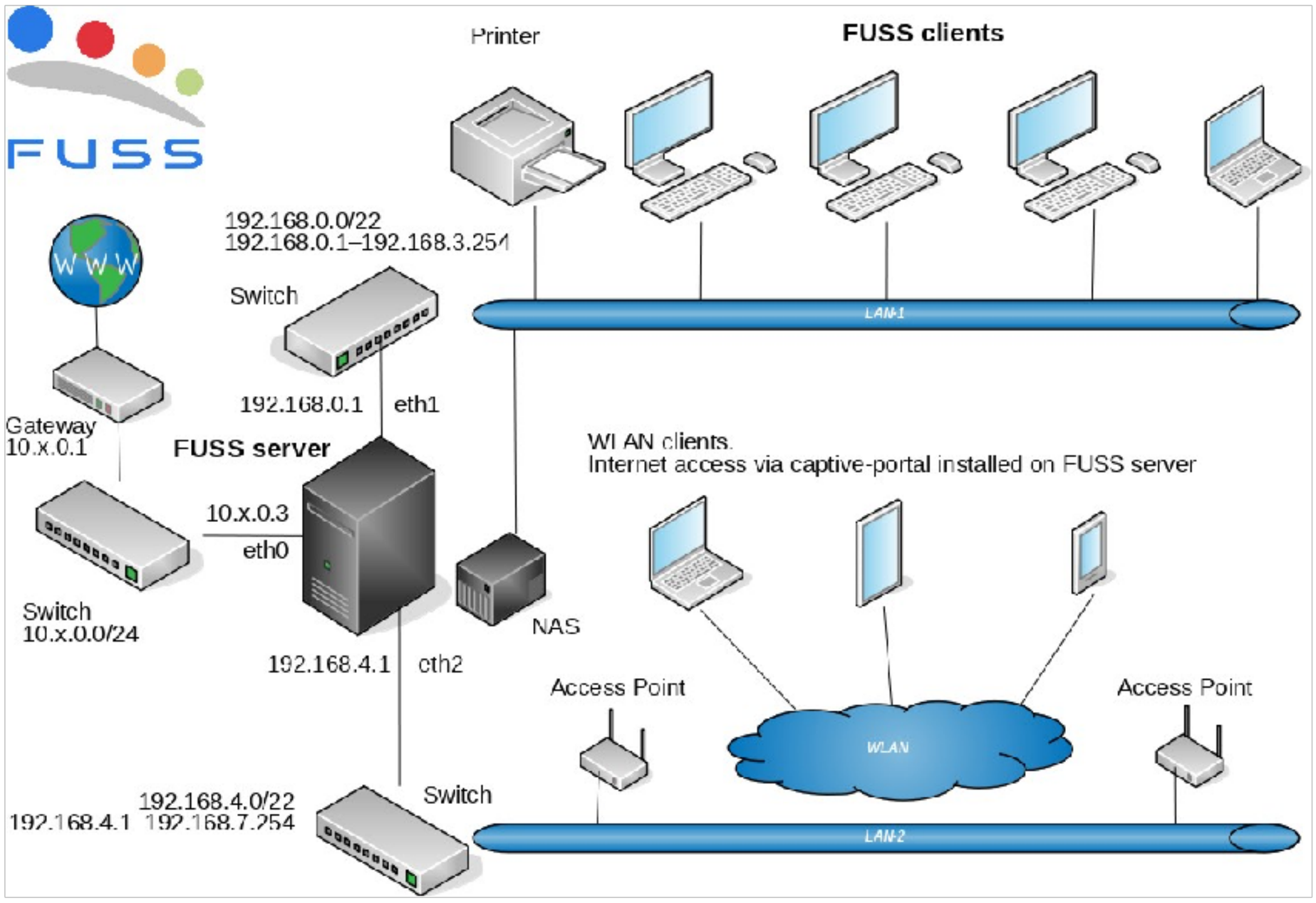


Fig. 1: Typical topology of a FUSS network.

A FUSS server must have at least 2 network interfaces. The first one is used to connect to the WAN (Wide Area Network) while the second one is connected to the local area network (LAN-1) in the school. The presence of a third Ethernet port on the server and a second LAN in the school to which WiFi access points are connected are prerequisites for being able to install a captive-portal on the FUSS server that offers the possibility for satellite devices to access the Internet after authentication.

1.2 Installation of FUSS server from the cloud-init template ready

Starting with version 10, a faster installation mode of the FUSS server is available from a preinstalled virtual machine image with support for cloud-init autoconfiguration technology.

This mode can only be used with a virtualization system; here it will be illustrated how to do so with the Proxmox virtualization platform, adopted by the project, which supports the indicated technology by allowing all features of the virtual machine to be managed directly from its web interface.

In particular, it becomes possible:

- Manage network addresses, gateways and DNS from the web interface
- Manage hostname and domain of the web interface
- Automatically enlarge the root disk once resized on the web interface

1.2.1 Virtual machine installation

The first step is to download the image prepared by the project to include it among the dumps available for restoration. This is available at http://iso.fuss.bz.it/cloud-init/vzdump-qemu-fuss-server-10-latest.vma.zst and the

easiest thing is to download it directly to the Proxmox server on which it will be used by connecting with SSH and running:

```
# cd /var/lib/vz/dump/
# wget http://iso.fuss.bz.it/cloud-init/vzdump-qemu-fuss-server-10-latest.vma.zst
```

Note: If you have configured storage other than `local` in Proxmox for dump images place us in the respective directory instead of under `/var/lib/vz/dump/`.

Note: newer images are compressed with `zstd` format and the file has `.zst` extension, some of the earliest images (the use of which is not recommended anyway) are in `lzo` format and have `.lzo` extension.

Once the download is complete the image will appear among in storage contents (from the web interface) and you can also start the restore directly from the interface by selecting it and using the "Restore" button which will create a new virtual machine on the first free VMID, the interface however allows you to indicate a different specific one. Be sure to indicate, again in the restore window, the use of `local-lvm` as the restore storage and put a check in the "Unique" box.

Keep in mind that for this to work smoothly you must have configured Proxmox to use FUSS, the virtual machine in fact assumes the presence of at least two different network interfaces, one on the external network (`vmbr0`) and one on the internal network (`vmbr1`); if this is not the case you can still change the interface assignments once the virtual machine is restored.

Alternatively, you can restore from the command line (assuming you have configured the storage to LVM with the name used in the default Proxmox installation) with:

```
qmrestore /var/lib/vz/dump/vzdump-qemu-000-0000_00_00-00_00_00.vma.zst \
   106 -storage local-lvm -unique
```

where any free VMID can be used instead of `106`. The storage must be local-lvm (like direct install), and the use of `-unique` allows you to generate a MAC address of the new VM that does not conflict with any others that may be present (this is unlikely unless you re-install multiple machines from the same source image, but it is a good idea to do so).

Once the image has been restored, it should be associated with the configuration disk image with:

```
qm set 106 --ide2 local-lvm:cloudinit
```

Note: If you get an error like:

```
lvcreate 'pve/vm-106-cloudinit' error:   Logical Volume "vm-106-cloudinit" already␣
↪exists in volume group "pve"
```

we remove the previous instance of the logical volume with:

```
lvremove pve/vm-106-cloudinit
```

And repeat the command.

At this point before booting the machine for the first time you can configure the network from the web interface, in the *Cloud-Init* section, setting: the IPs on the network interfaces, the default gateway for the external interface, an SSH root access key, the domain and DNS server. The latter must always be `127.0.0.1`, and the domain name must be the one that will later be used in the final configuration performed by the `fuss-server` command.

Warning: you must **always** configure the DNS server as `127.0.0.1` and the domain name ugua- le with the one that will be used later with the `fuss-server` command otherwise there is a risk that in a subsequent execution of `fuss-server`, or in re-executing the initialization of cloud-init, there will be mutual interference and overwriting

All of these operations can also be done at the command line; to enter the above parameters into the `cloud-init` configurations (tailor the network addresses to your needs) run:

```
qm set 106 --ipconfig0 ip=10.0.101.79/24,gw=10.0.101.1
qm set 106 --ipconfig1 ip=192.168.0.1/24
qm set 106 --searchdomain fusslab.blz
qm set 106 --nameserver 127.0.0.1
qm set 106 --sshkey ~/.ssh/id_rsa.pub
```

the last command, if you have a list of keys, can be replaced by:

```
qm set 106 --sshkey listchiavissh.txt
```

where `listchiavissh.txt` is a file containing the list of public keys (one per line) that will be enabled for the machine in question; you can generate it from a list of key files with something like `cat *.pub > listchiavissh.txt`.

In addition to the network configuration, the machine hostname should also be set from the web interface. This corresponds by default to the name used by Proxmox for the relevant VM (the one shown along with the VMID in the interface). In the distributed image, `fuss-server-base-image` was used as the default name, which can be changed in the *Options* section of the web interface. Again, the change can be made at the command line with:

```
qm set 106 --serverhostname
```

Warning: although you can set the machine hostname later within the machine with `hostnamectl`, since the initial network configuration is handled by cloud-init anyway, you should configure the hostname directly in this section and it will also be correctly propagated in the various configurations.

Warning: keep in mind that if you change any of these parameters at a later time, **all** the configurations managed by it will be regenerated by cloud-init on the next reboot. This also includes the SSH keys of the server, with the consequence that the previous ones will no longer be valid; so if you have already connected to the machine you will get the usual warning that the fingerprints of the server keys do not match, and you will need to remove them and accept them again.

You will also have to modify the hardware parameters of the virtual machine (from the *Hardware* section of the same name in the Web interface), to increase the memory and enlarge the disk as much as necessary, and possibly add missing network interfaces (for example, the one for the captive portal). You will also have to enable automatic startup of the virtual machine at boot time, from the *Options* section. Even to change these features you can continue to operate directly at the command line, with something like:

```
qm set 106 --memory 4096
qm set 106 --onboot 1
qm resize 106 scsi0 500G
```

where you increase the RAM assigned to the virtual machine to 4G, require automatic launch on Proxmox reboot, and enlarge the disk to 500G. If, however, you decide to dedicate a separate disk for home this last operation does not have to be performed, unless the 32G assigned in the default image to the root disk is insufficient, in which case however you perform it with an appropriate size.

The provided images already have discard enabled on the installation disk (the latter option only makes sense if, as in the example, you have a disk that was extracted from a storage that supports discard, such as LVM-thin), if it is absent or unnecessary you can enable/disable it respectively with:

```
qm set 106 --scsi0 local-lvm:vm-106-disk-0,discard=on
qm set 106 --scsi0 local-lvm:vm-106-disk-0,discard=off
```

Keep in mind that the given options will be applied on the next reboot, even for the disk enlargement part, which will be performed automatically by `cloud-init` (with the caveat, however, that this is only possible due to the specific partitioning used by the image provided by the project).

At the end of the first boot of the virtual machine, fingerprints of the generated keys for the SSH server are shown in the console (accessible from the inter- web face of Proxmox), which you can use to verify their correctness on the first connection. You can find them later in the `/var/log/cloud-init-output.log`.

1.2.2 Post-installation configurations

Once the installation is finished, it is generally not necessary to perform any other configuration, unless you need to keep the home on a separate disk, which is a good practice should you need to maintain disk quotas, and which will allow, in the future, to perform an upgrade just for the system part, without having to reinstall the files in the home.

However, the ability to have automatic disk resizing as is the case with t h e root filesystem is lost in this case, as cloud-init handles this functionality only for the latter. Since there are pros and cons we leave the evaluation of the use of separate homes to the person performing the installation, we will, however, discuss here how to configure separate disk homes.

Creating an additional disk for home

To install home on a separate disk, you arrange to add an appropriately sized disk to the virtual mac- china from the web interface ("Hardware" section, "Add->Hard Disk"). You can perform the same operation from the command line with something like:

```
pvesm alloc local-lvm 106 '' 100G
qm set 106 --scsi1 local-lvm:vm-106-disk-1,discard=on
```

(again, the `discard=on` option only makes sense if you are using storage such as `local-lvm`).

At this point once you boot the disk server it will be seen at boot as `/dev/sdb`. Log in as root and verify that the disk is actually recognized as `/dev/sdb`; at this point you will need to partition it and create the filesystem for home, this can be done with:

```
echo "start=2048, type=83" | sfdisk
/dev/sdb mkfs.ext4 /dev/sdb1
```

you retrieve the UUID of the disk and add it to `/etc/fstab`, this can be done with:

```
echo -e "# /home was on /dev/sdb1 during installation" >> /etc/fstab
echo -e "$(blkid -o export /dev/sdb1|grep ^UUID=) /home ext4 defaults,grpquota,
↪usrquota 0 2" >> /etc/fstab
```

Replace `/dev/sdb1` with the appropriate device file if another one was used. Aside from adding an explanatory comment, the command extracts the UUID of the newly created filesystem and creates a correct home entry with options to have quotas and the correct sequence number in the initial filesystem check scan.

Once you have verified that there are no files or directories under `/home in` the cloud-init installation (there may remain the home of the `debian` installation helper user, which can be removed with `userdel -r debian`) you can mount the home disk with `mount -a`.

Initial configuration for quotas

Whether you used an additional disk for `/home` or later enabled quotas on the root (by adding `grpquota,usrquota` to its entry in `/etc/fstab`) you need to initialize quotas with:

```
quotacheck -a -f
quotacheck -ag -f
```

where the `-f` option is needed if (as is the case if you add mount options for dimensions on the root) to force the writing of the dimension files when the system is active. Warnings that the data may be inaccurate can be ignored; they will still be corrected on the first restart.

Once quotas are active you can use the `repquota` and `repquota -g` commands to verify the actual presence of quotas. If said commands are not present you can install them with `apt install quotatool` (they were included in the cloud-init image anyway).

If you do not restart the machine after running the previous commands and activating the quotas in the mount options, or if you add the `grpquota,usrquota` options later by remounting the filesystem, and force the calculation of quotas with the filesystem mounted also using the `-m` option with the previous two commands, you will also need to activate the quotas explicitly with:

```
quotaon -a
```

1.3 Installation of FUSS server traditional

To install FUSS Server on a physical machine, you must start with an installation of Debian Bookworm, on which the FUSS server is based. Images can be obtained from the address

https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/ by taking

the file `debian-<version>-amd64-netinst.iso`.

For *installations in Bolzano schools* this image will need to be *uploaded to the proxmox server* previously configured, then continuing with the creation of the virtual machine until it boots. But in this case it is preferable to use the procedure outlined in the previous paragraph.

Instead, to install directly to the server, you need a USB flash drive with a minimum capacity of 1 GB to which the downloaded ISO image should be copied. In GNU/Linux you can use the `dd` command. After inserting the flash drive into the PC where the image is available, check with the `lsscsi` command which device has been assigned to the flash drive. In the example we use `/dev/sdX` where X can be any of the letters `a`, `b`, `c`, etc. As root, give the command:

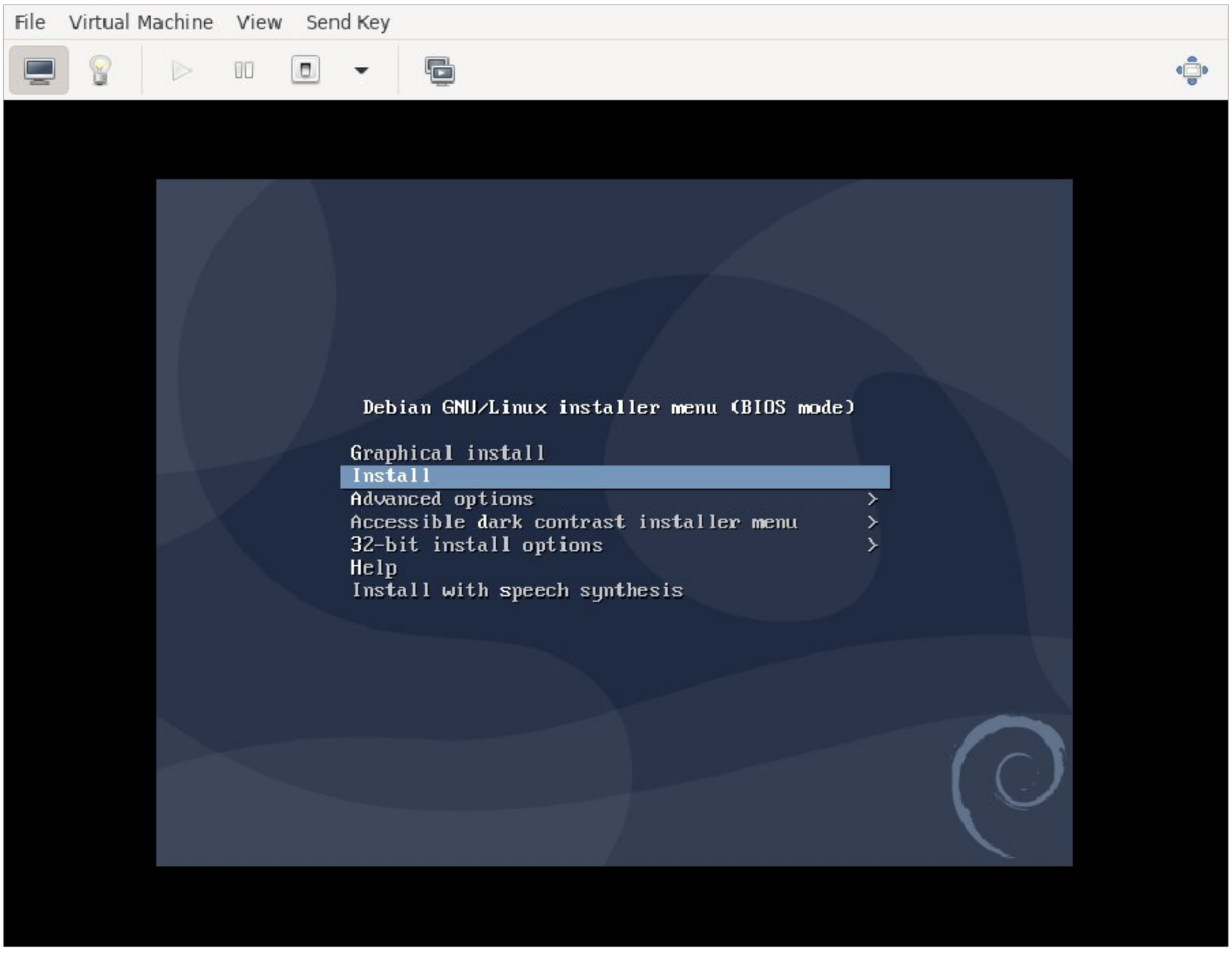
```
# dd if=/PERCORSO_IMMAGINE/fuss-server-8.0-amd64-201708221233.iso \
  of=/dev/sdX bs=4M status=progress
```

Having prepared the USB flash drive, insert it into the server and after starting it, be sure to choose the flash drive itself as the boot device.

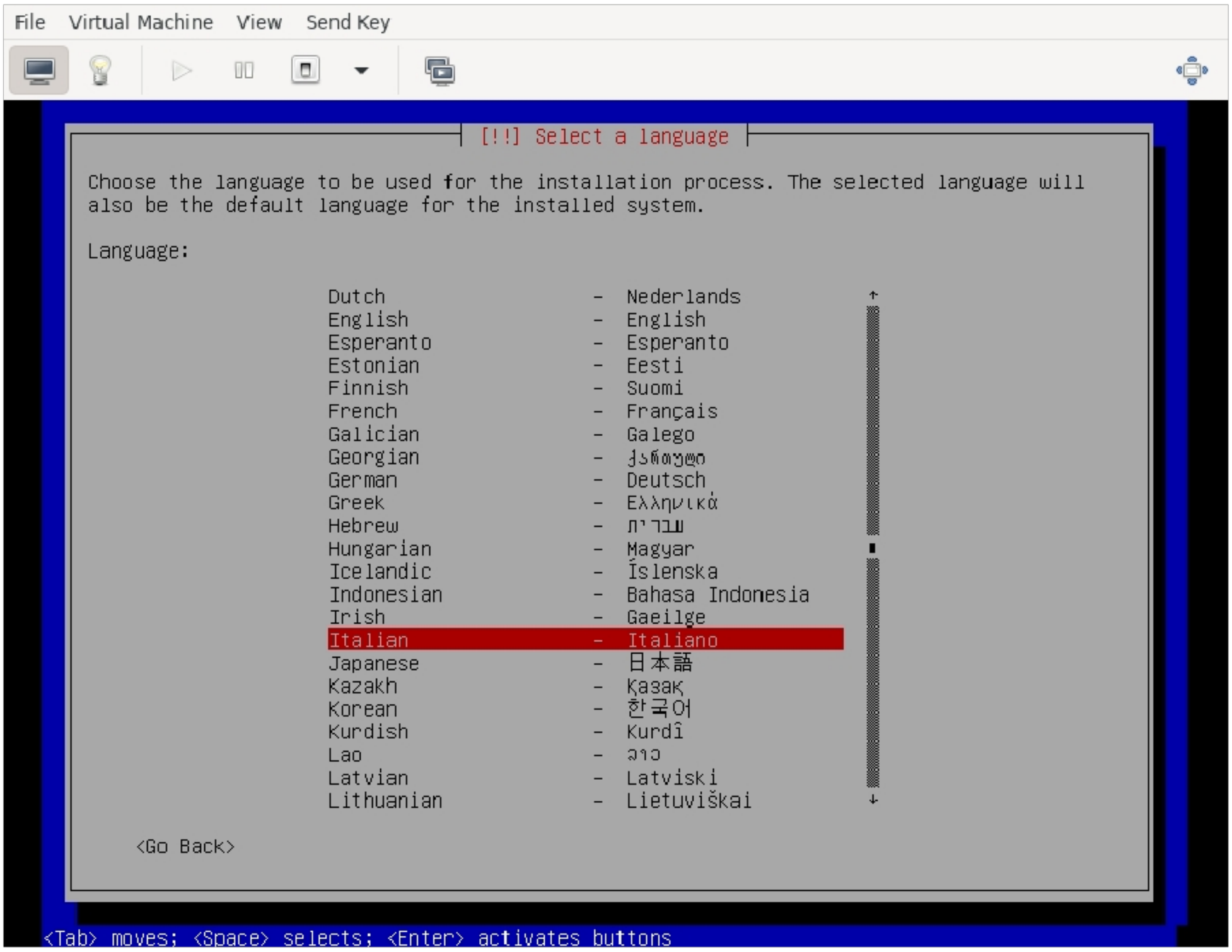
1.3.1 Installation of Debian

Initial configurations

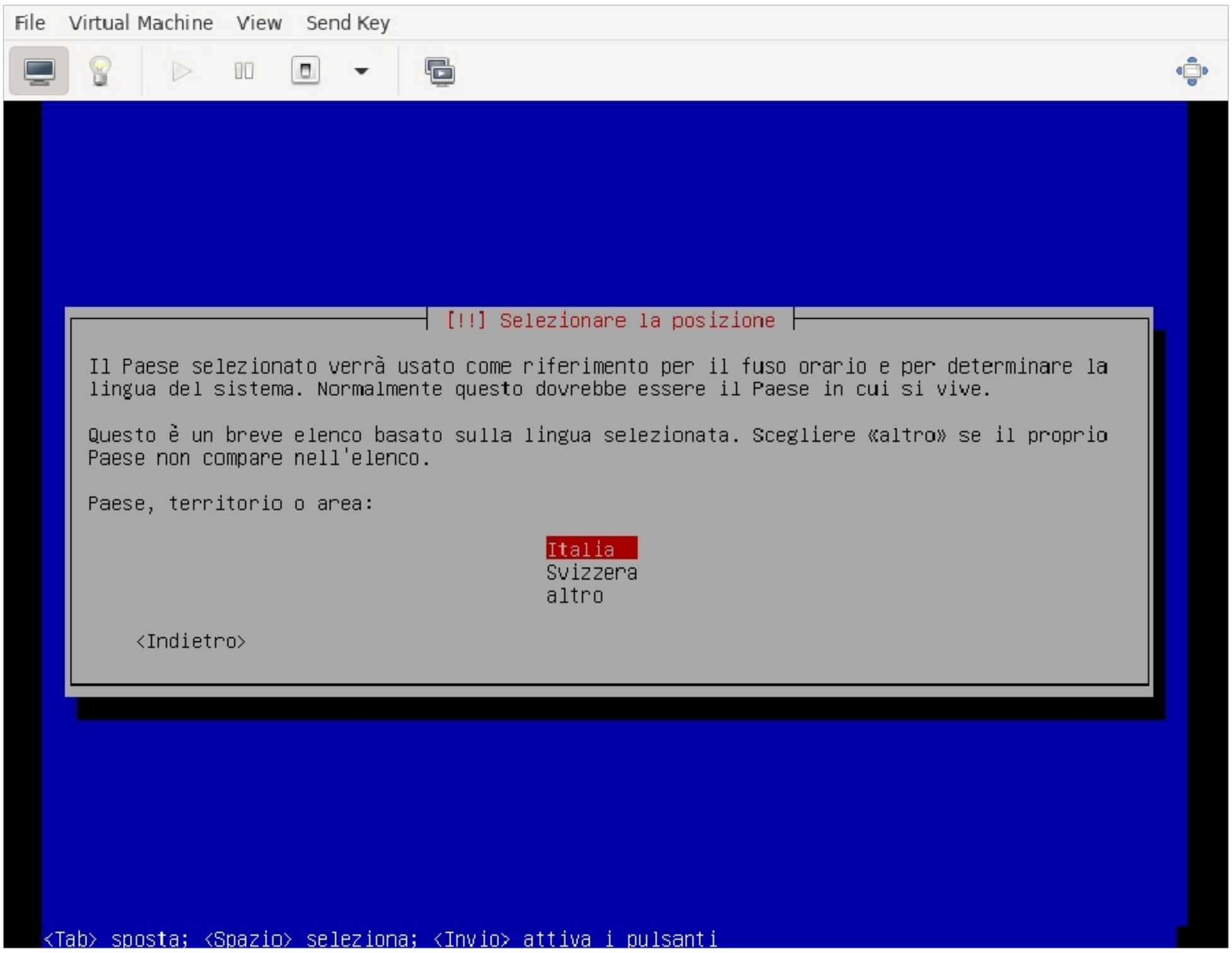
If you have correctly configured virtual machine booting from the Netinstall ISO you will get the following initial screen:



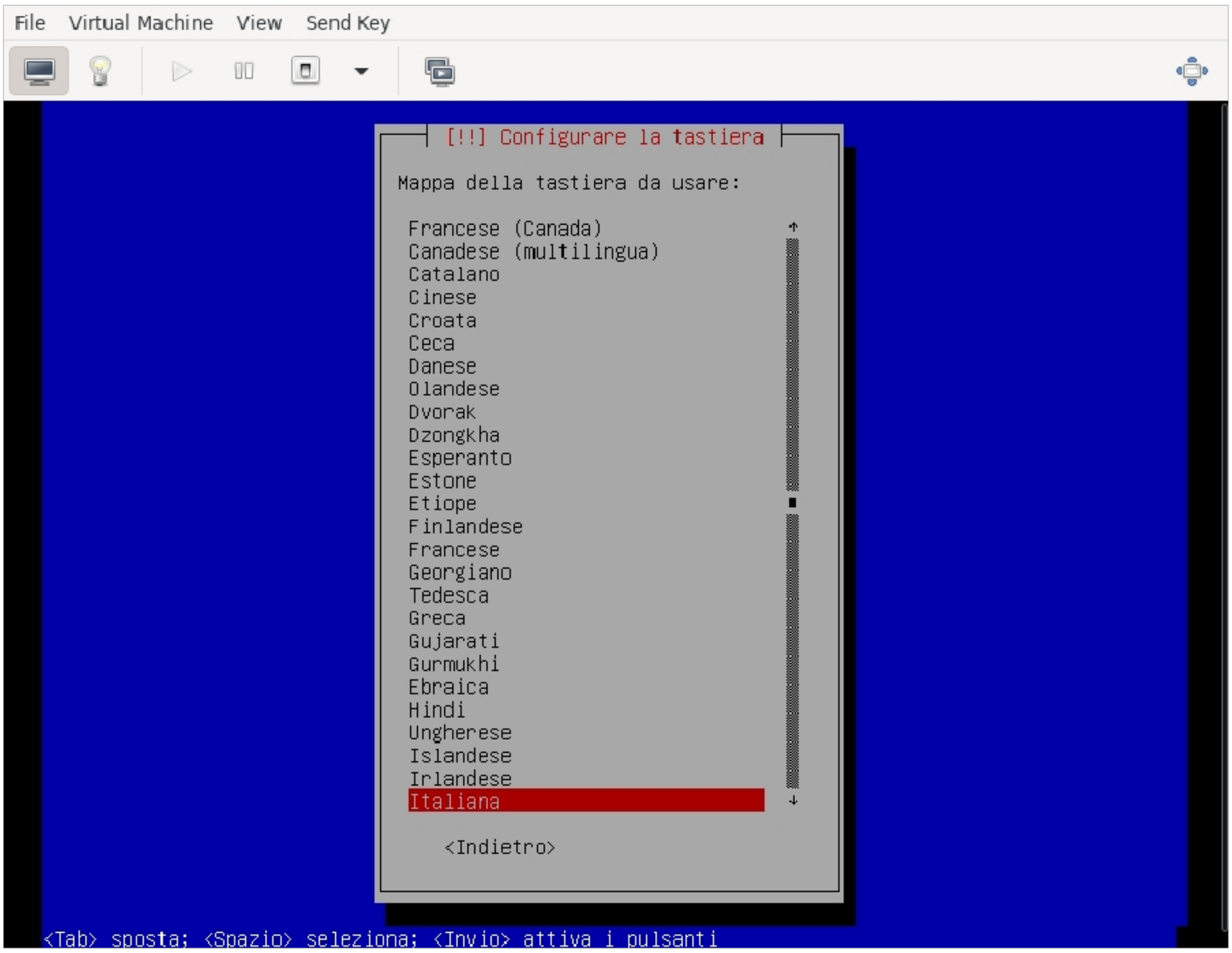
you choose a text installation, you will be asked in order for the language:



and choose Italian; location (for time zone):

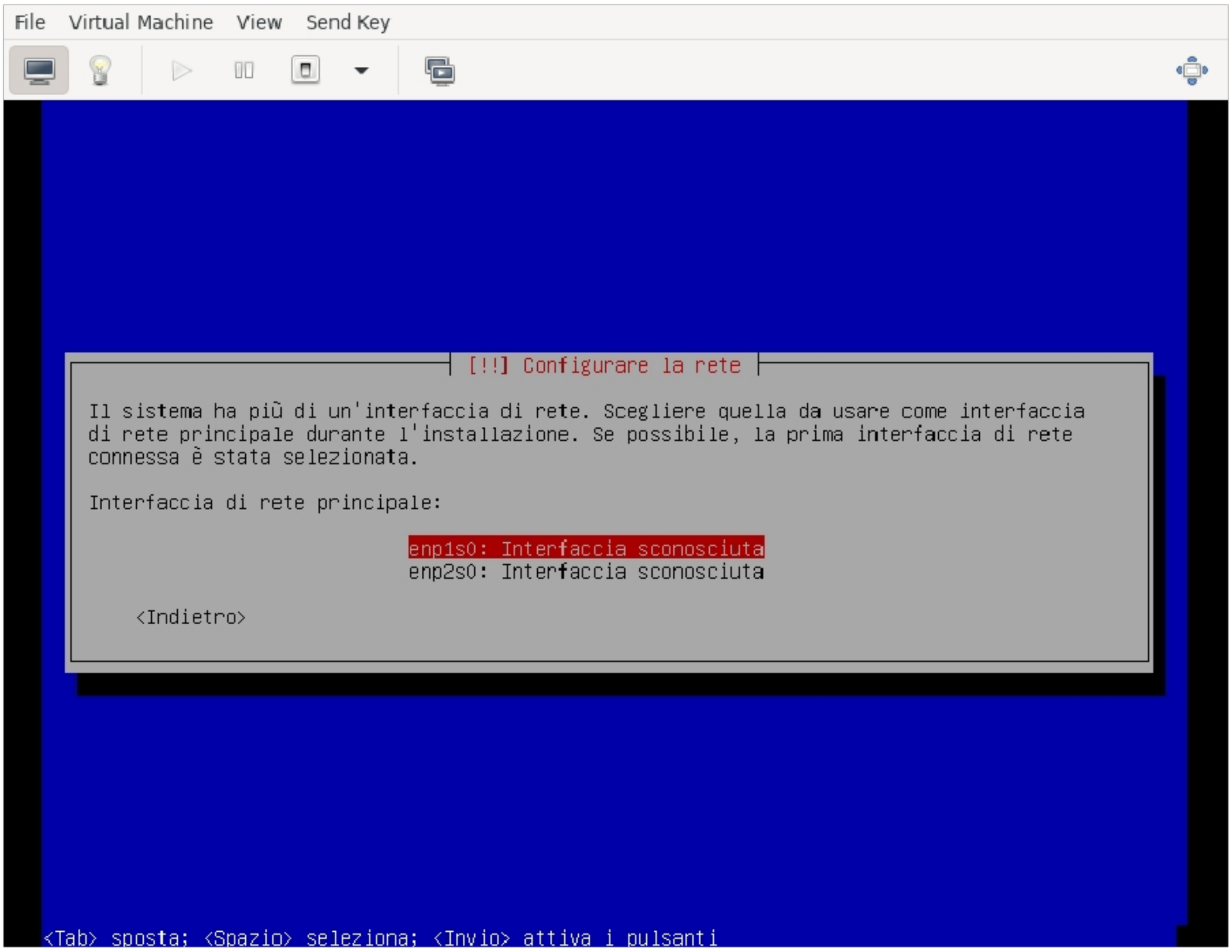


And Italy is chosen; the keyboard:

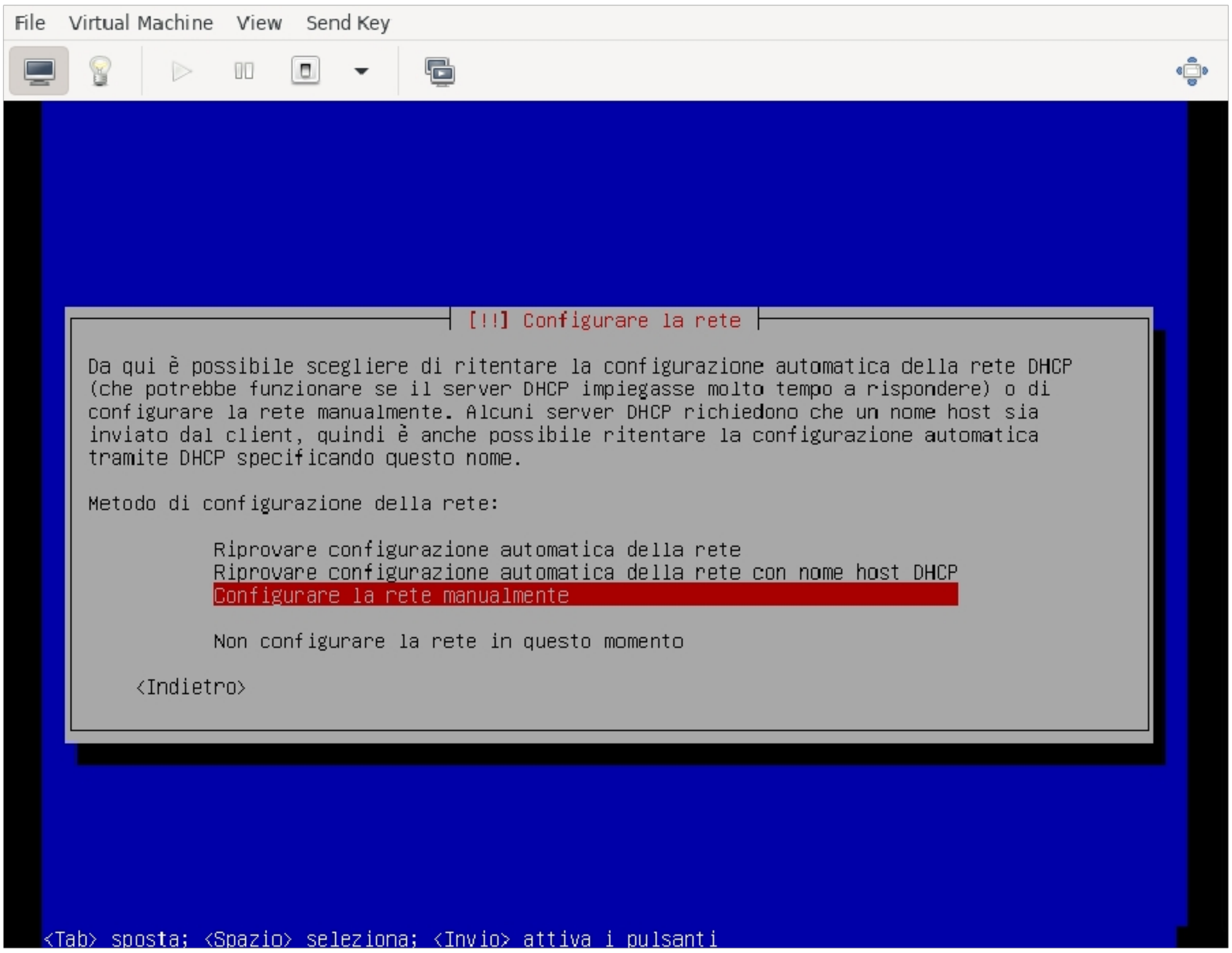


And you choose the Italian one.

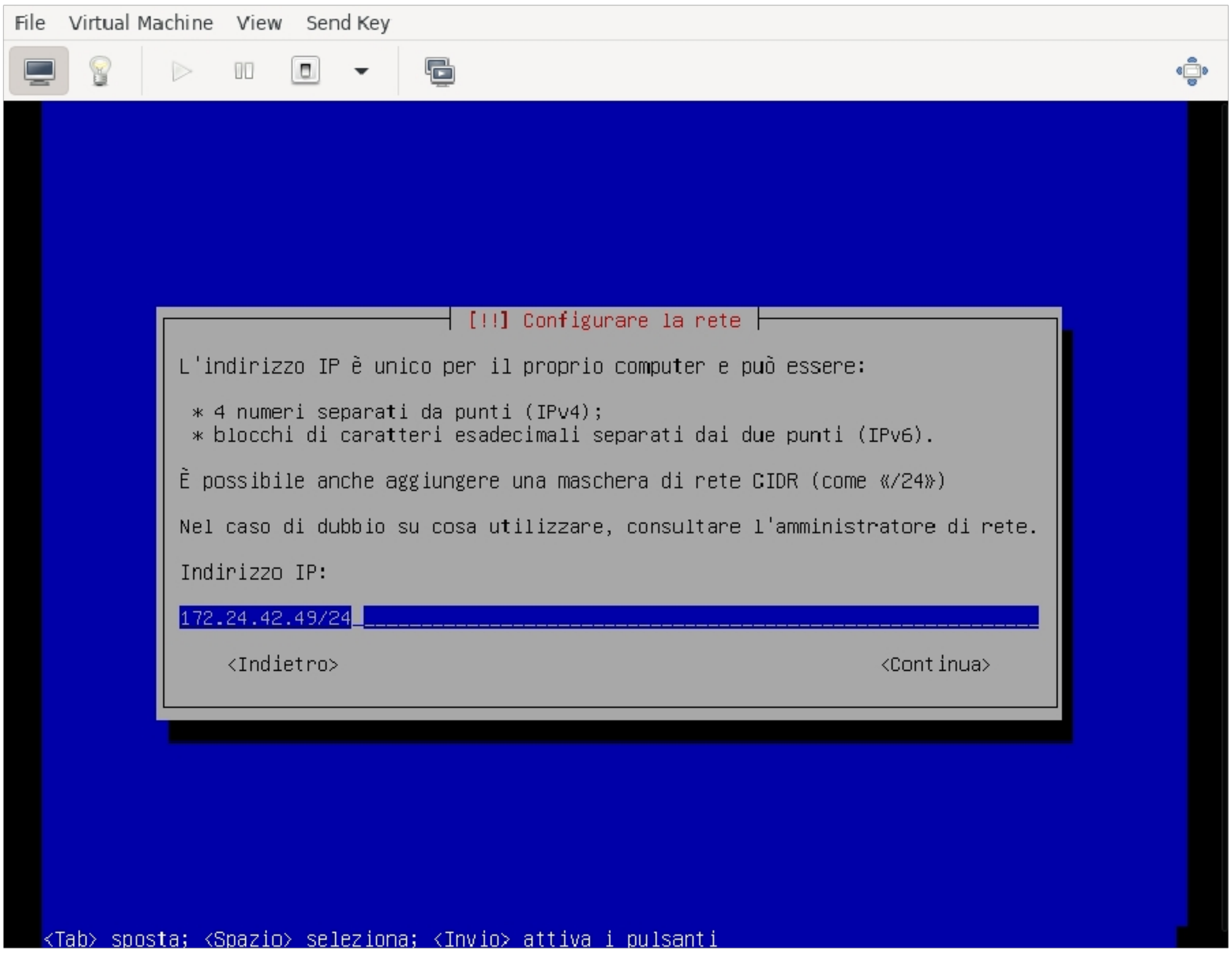
For the network, use the one corresponding to the server's WAN (the one facing the Internet) as the interface for installation:

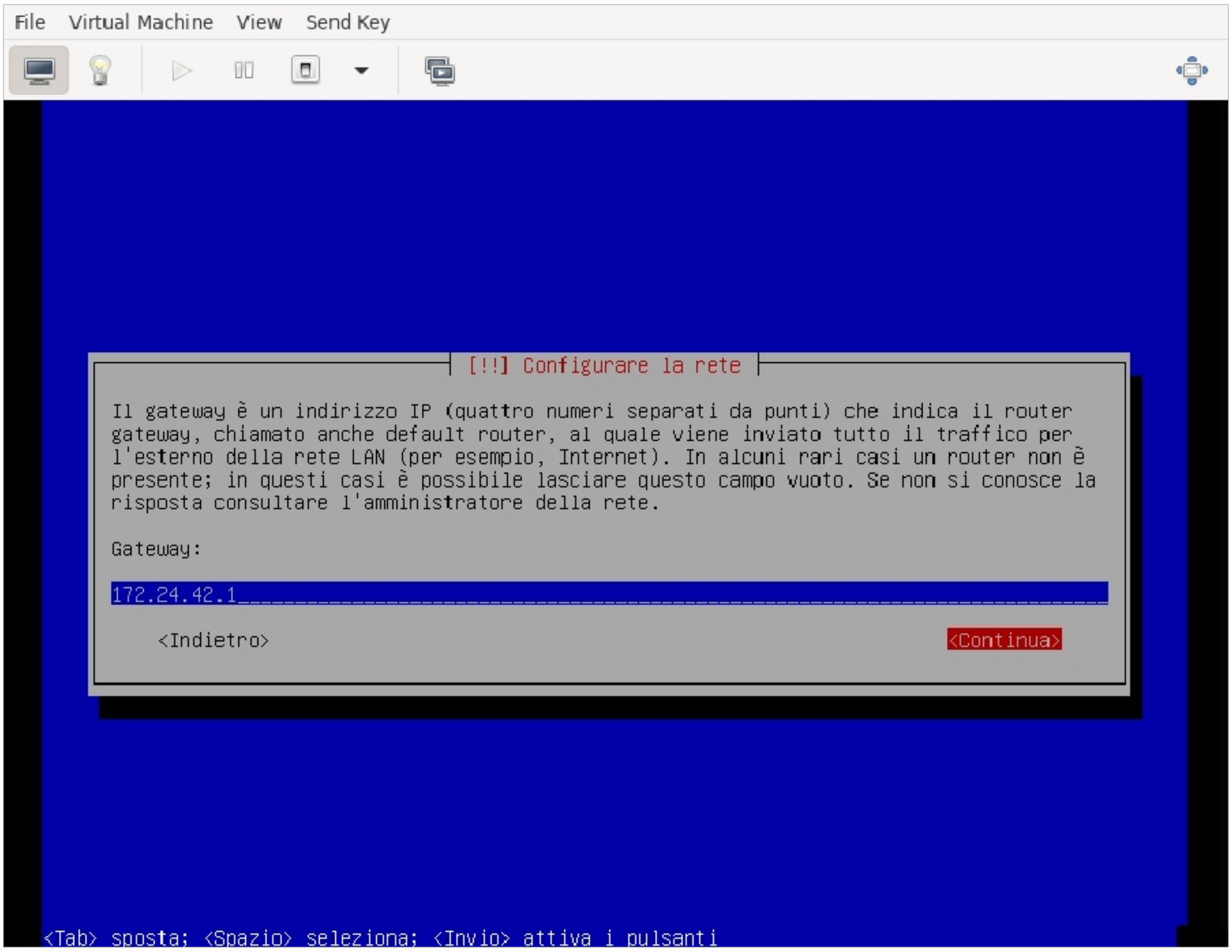


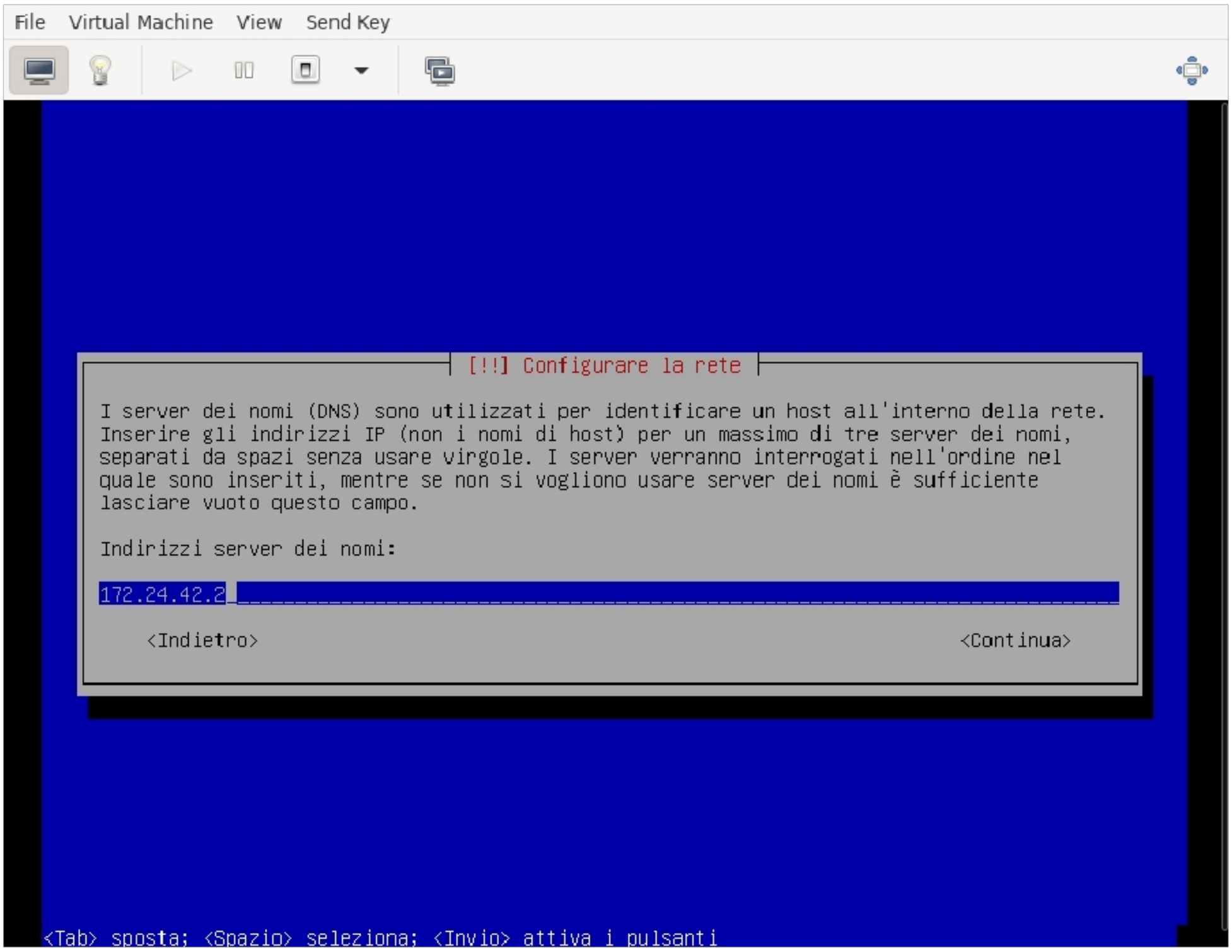
the installer will attempt automatic configuration of the network, which must be aborted (press enter during acquisition to cancel it, or go back if it has been done). This will allow you to explicitly select a manual configuration for the "external" IP of the fuss-server:



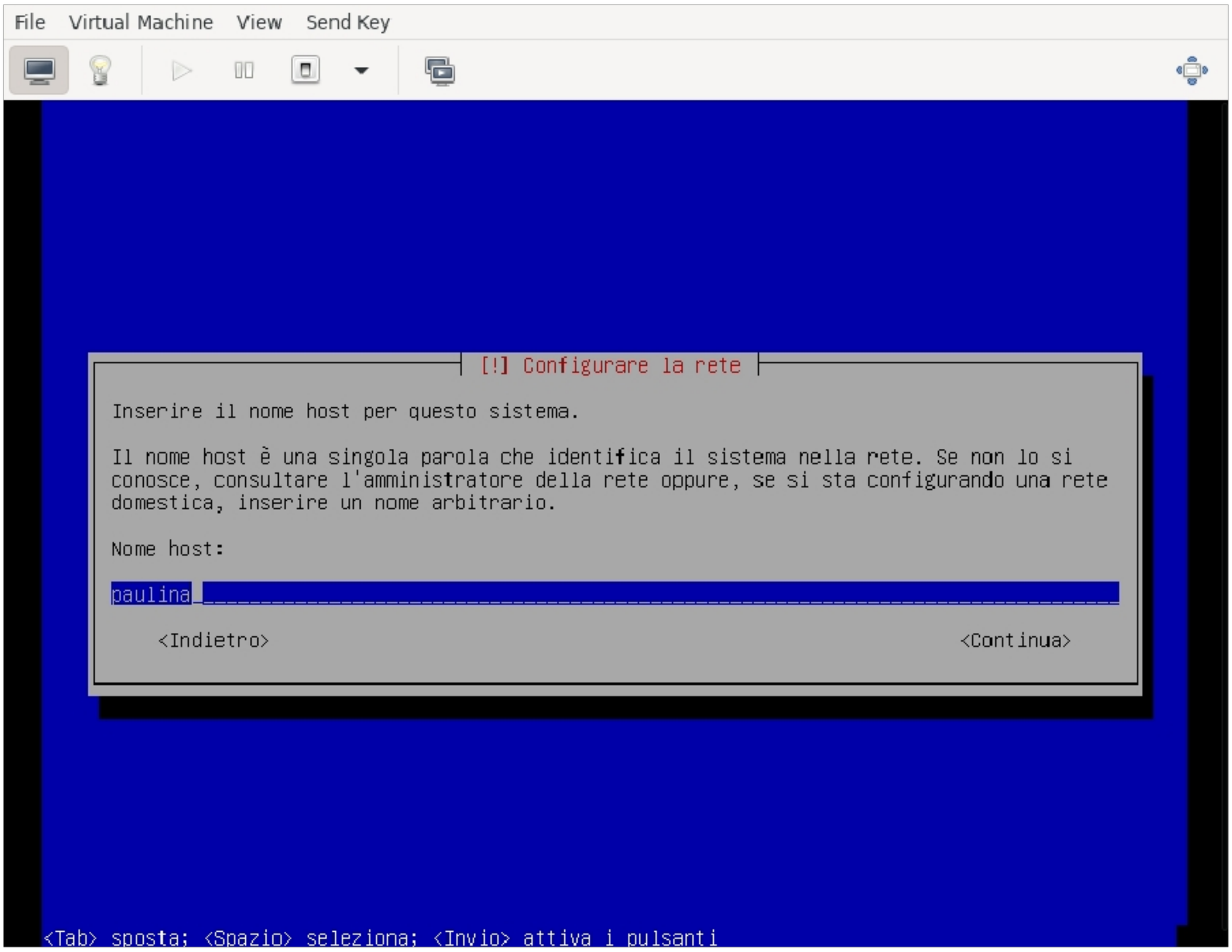
and make the standard network settings (IP address, netmask and default gateway and DNS):


File Virtual Machine View Send Key
[!!] Configurare la rete
L'indirizzo IP è unico per il proprio computer e può essere:
* 4 numeri separati da punti (IPv4);
* blocchi di caratteri esadecimali separati dai due punti (IPv6).
È possibile anche aggiungere una maschera di rete CIDR (come «/24»)
Nel caso di dubbio su cosa utilizzare, consultare l'amministratore di rete.
Indirizzo IP:
172.24.42.49/24
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

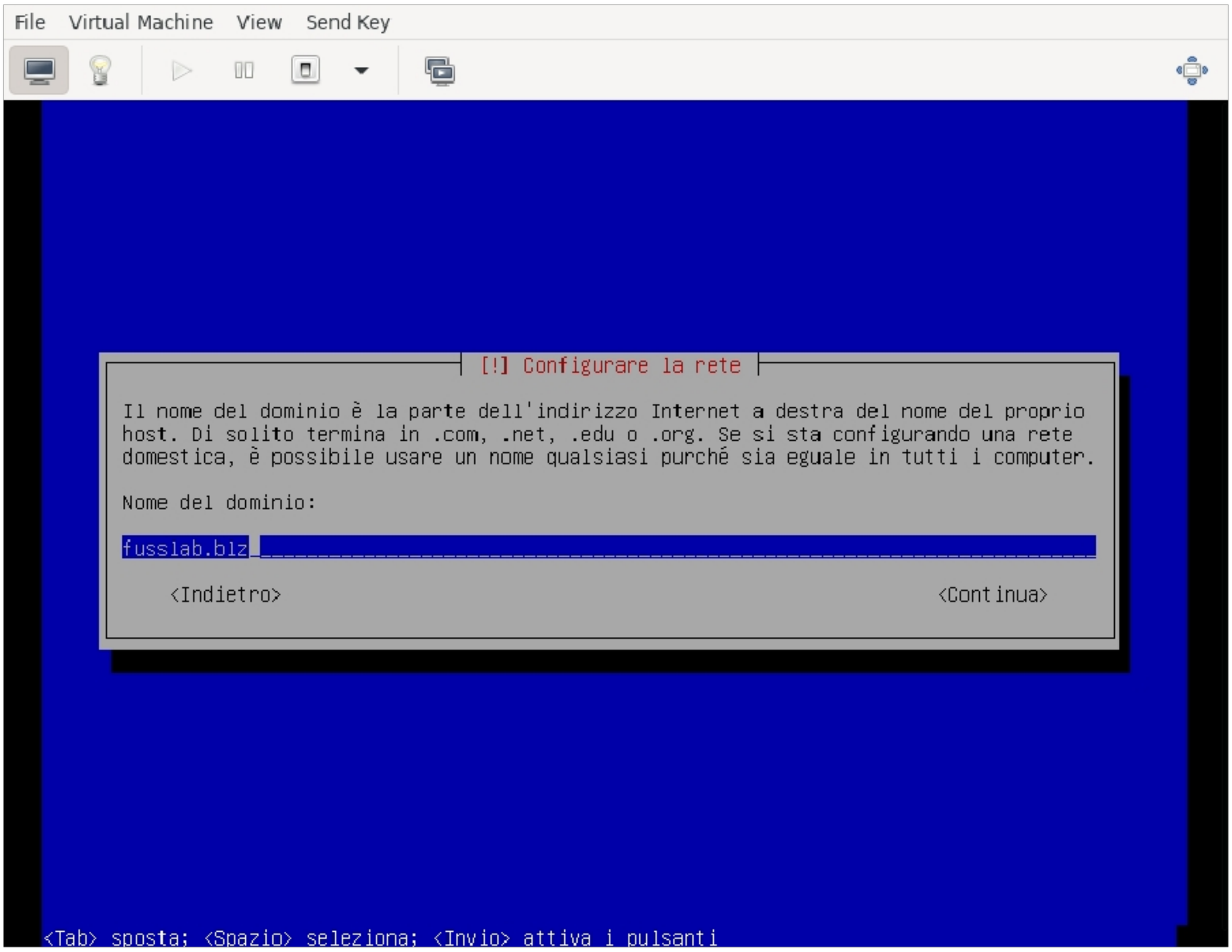

File Virtual Machine View Send Key
[!!] Configurare la rete
Il gateway è un indirizzo IP (quattro numeri separati da punti) che indica il router gateway, chiamato anche default router, al quale viene inviato tutto il traffico per l'esterno della rete LAN (per esempio, Internet). In alcuni rari casi un router non è presente; in questi casi è possibile lasciare questo campo vuoto. Se non si conosce la risposta consultare l'amministratore della rete.
Gateway:
172.24.42.1
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti



You will then be asked for the name of the machine; enter the final one now:



you then continue by setting up the domain:



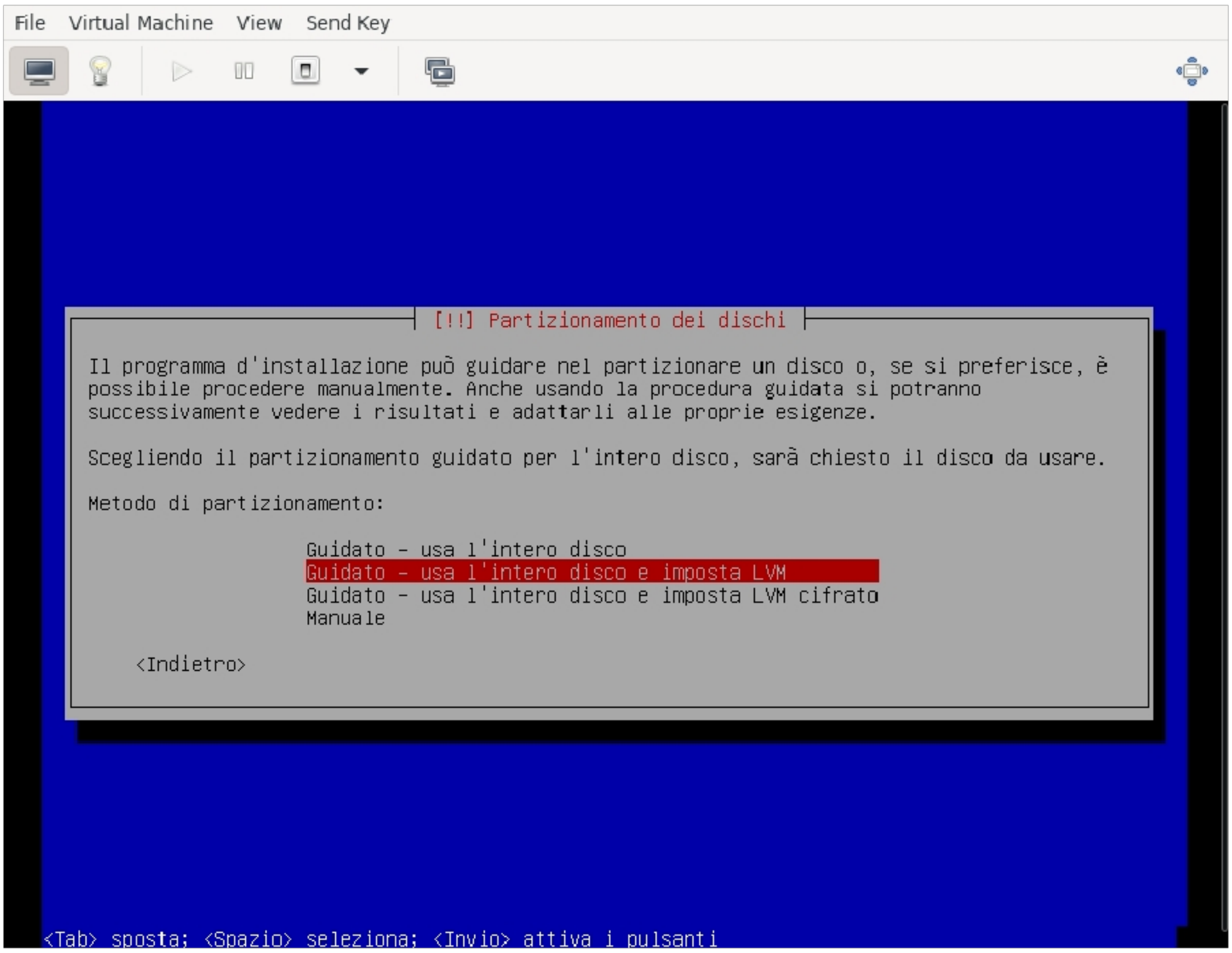
You will then be asked for the root password and initial user, which you can set as

desired. You will then have to perform disk partitioning for the system installation.

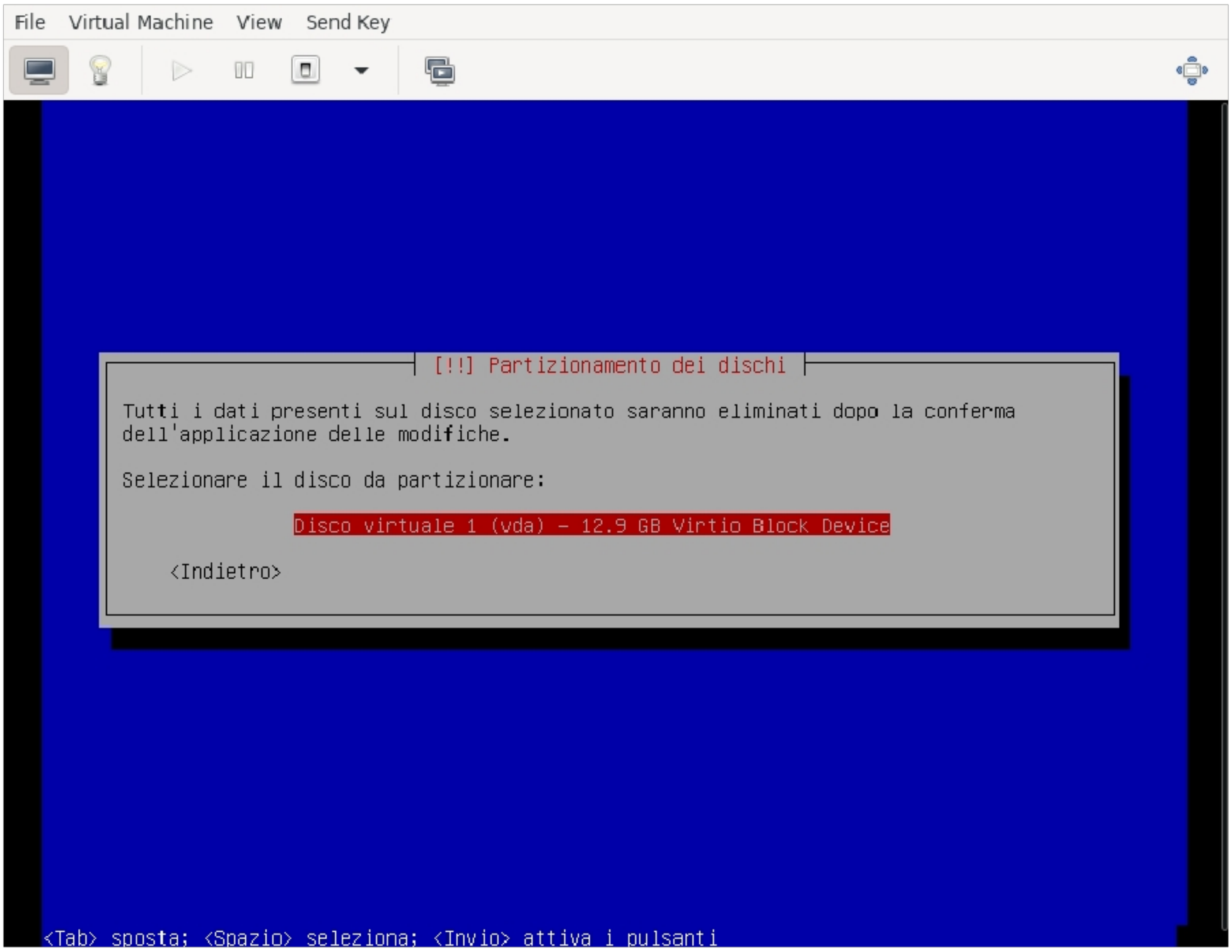
The safest choice, to avoid root-filling problems, is to use separate filesystems for `/home`, `/var`, `/tmp`. However, this with direct partitioning makes the eventual reallocation of disk space less flexible.

In fact, keep in mind that even if you have available disk space to be able to enlarge partitions, the enlargement would occur on the "bottom" therefore it would be easy to resize only the last partition (in the case of the `/home`, which while being the most likely one, is not necessarily really the one that needs the additional disk space).

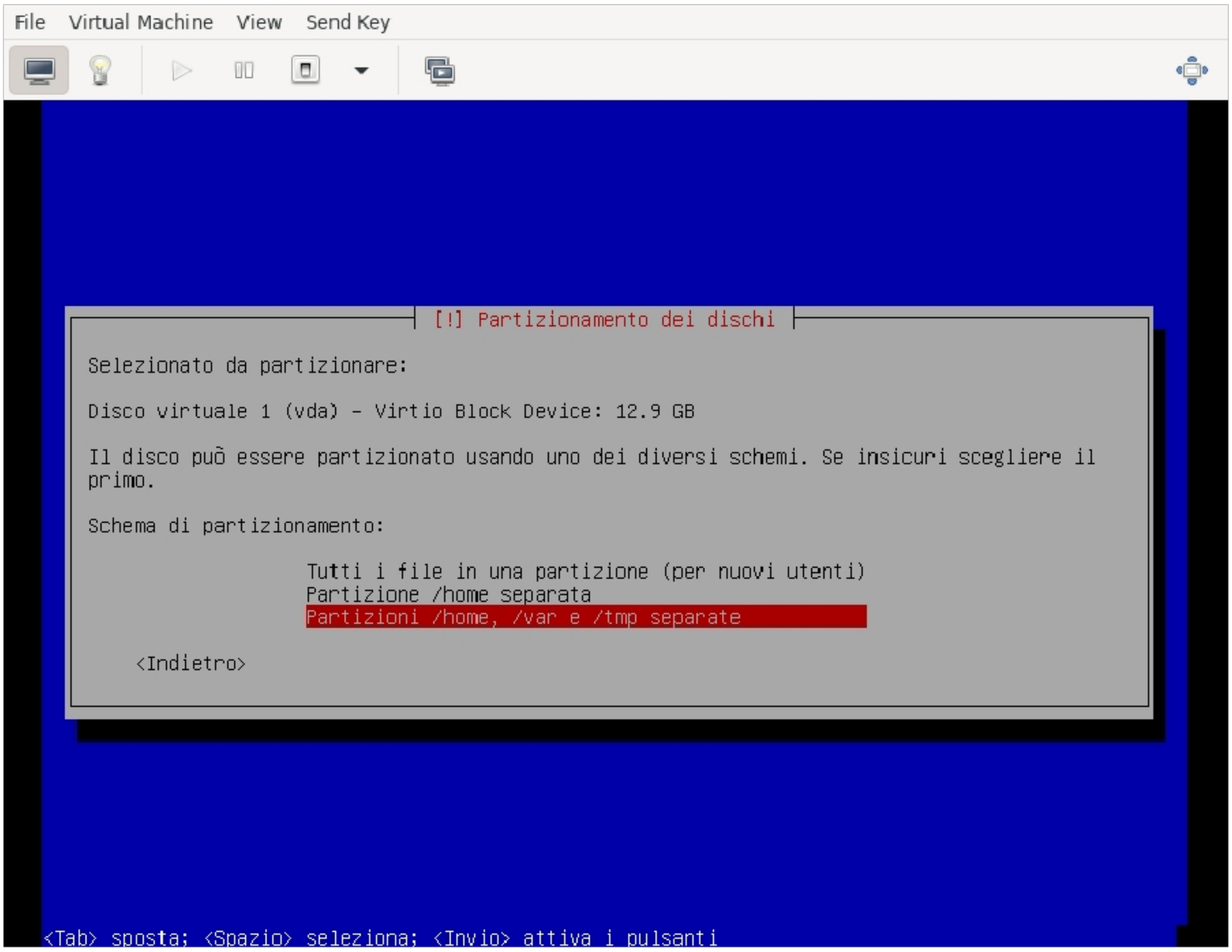
Therefore, it is suggested, for more flexibility at the cost of a slight loss of performance in I/O, to install using LVM, selecting "guided - use full disk and set LVM."



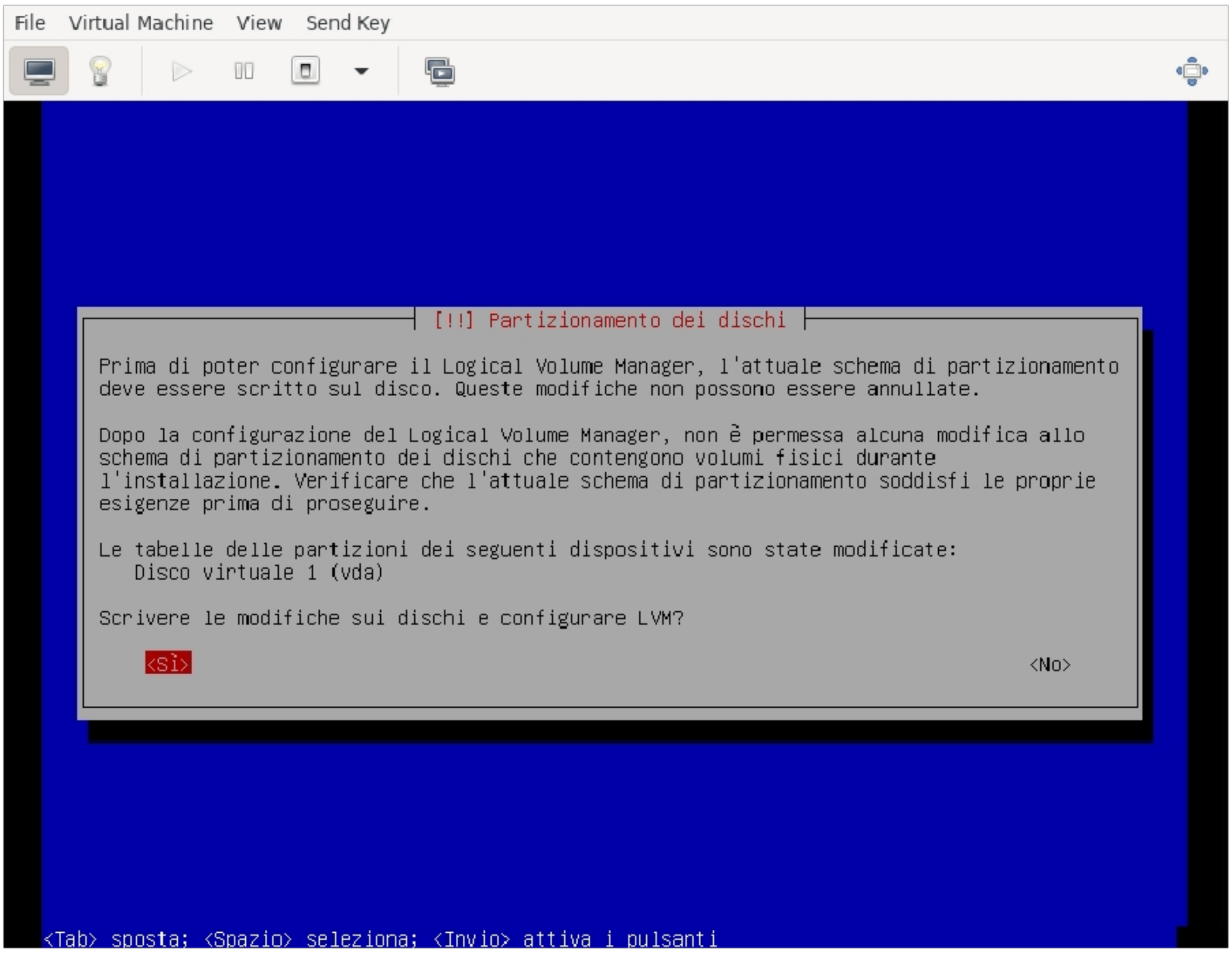
then select the disk to be partitioned:



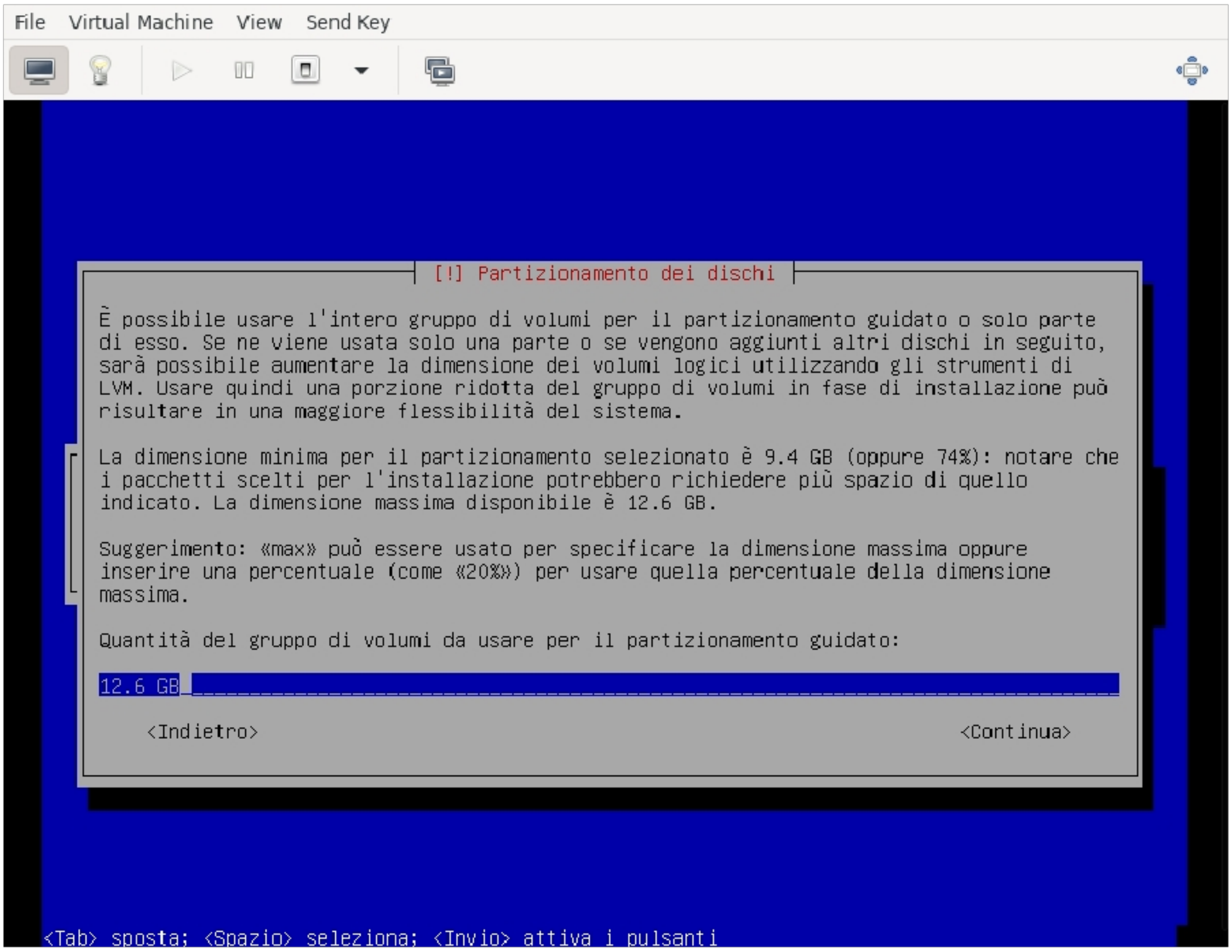
The use of separate filesystems:



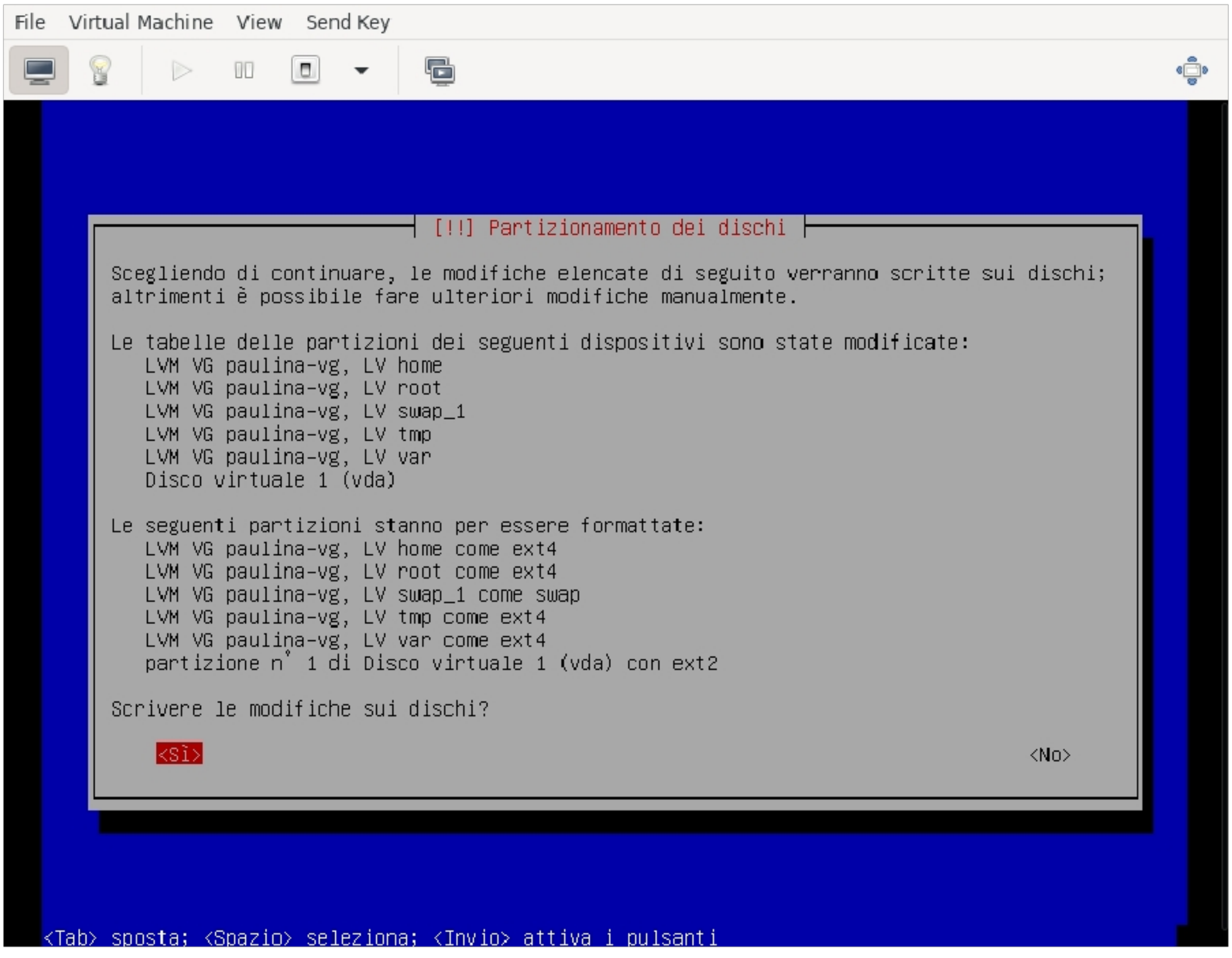
and confirm the configuration of LVM:



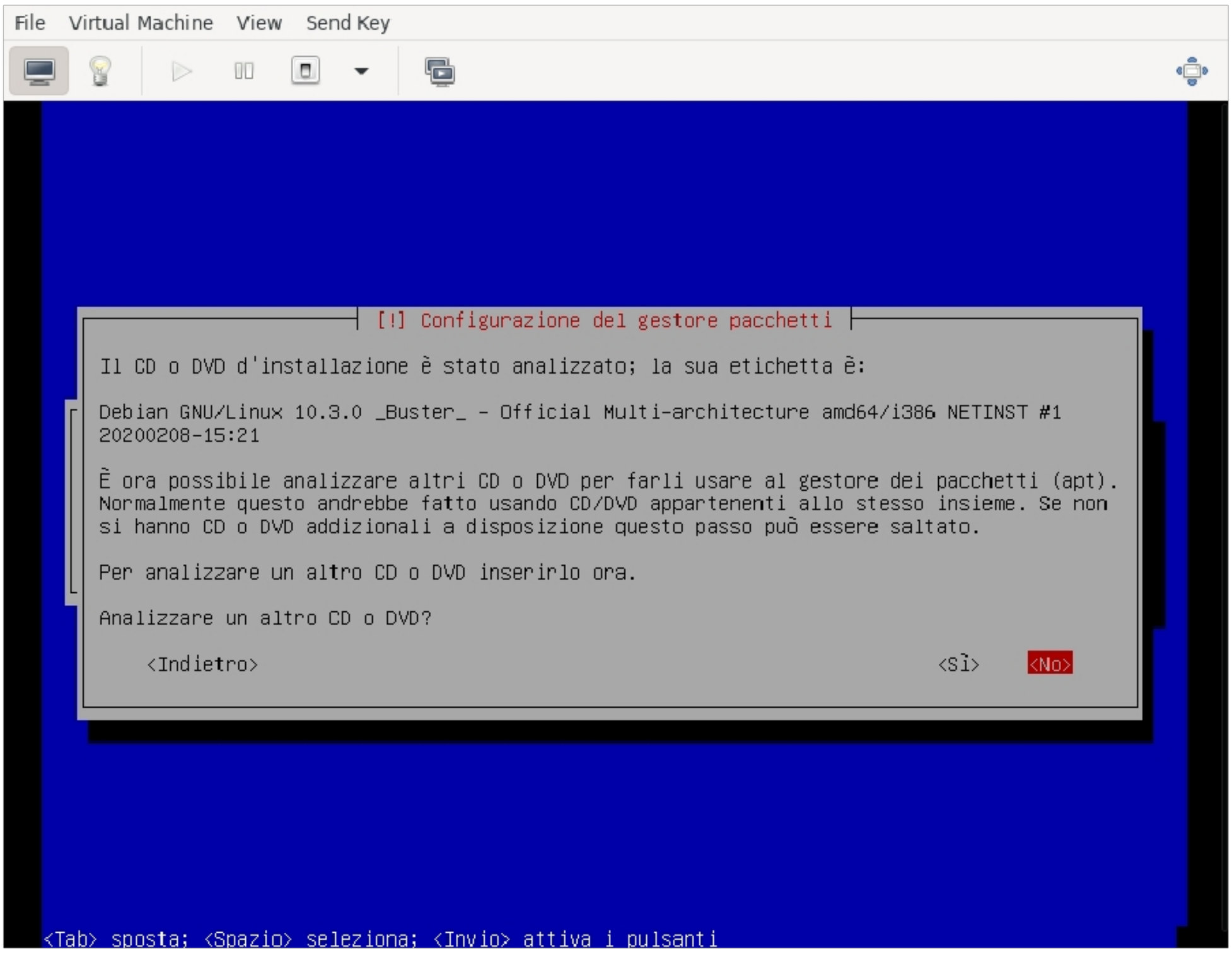
and the use of all available space for the volume group:



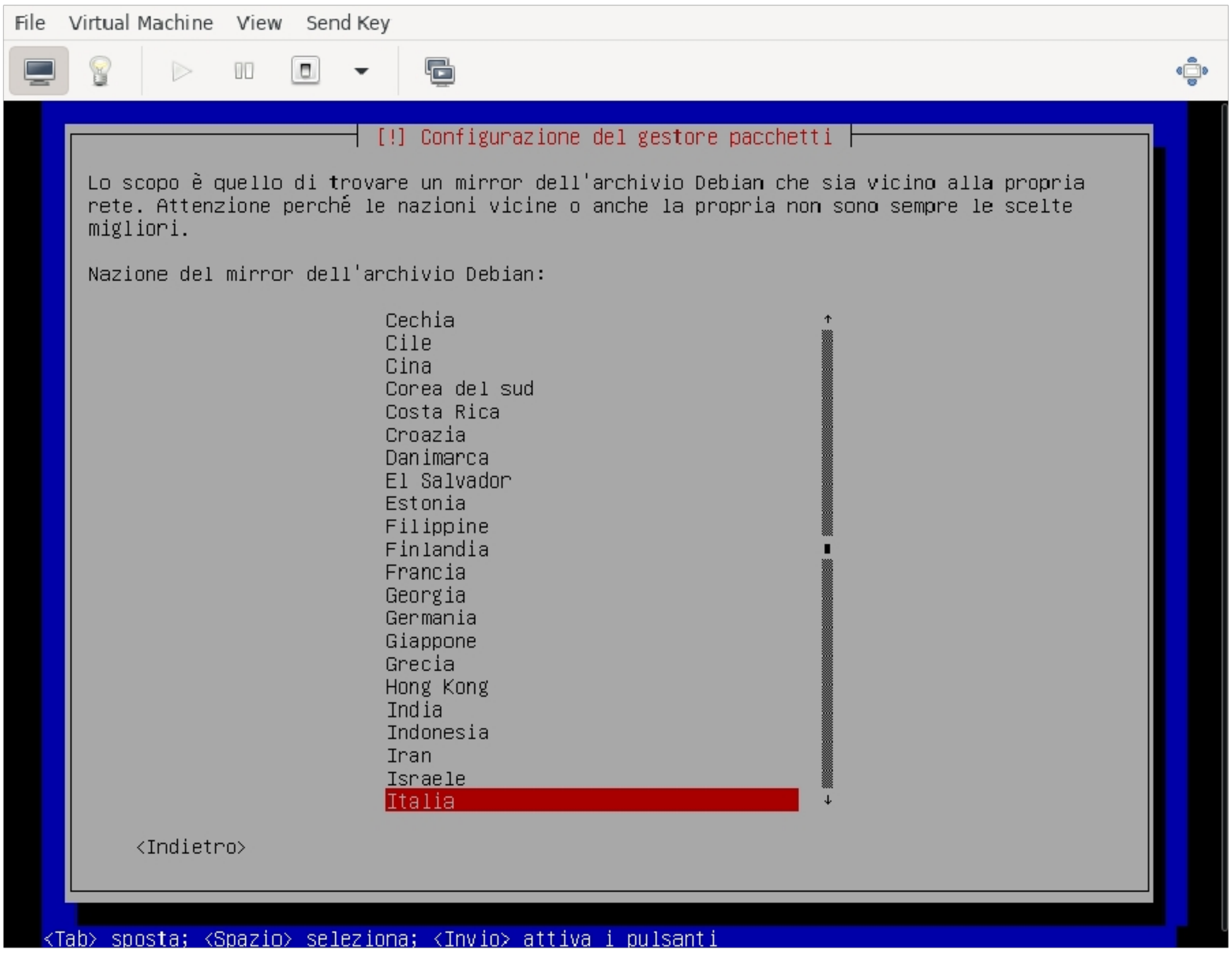
And then the final formatting:

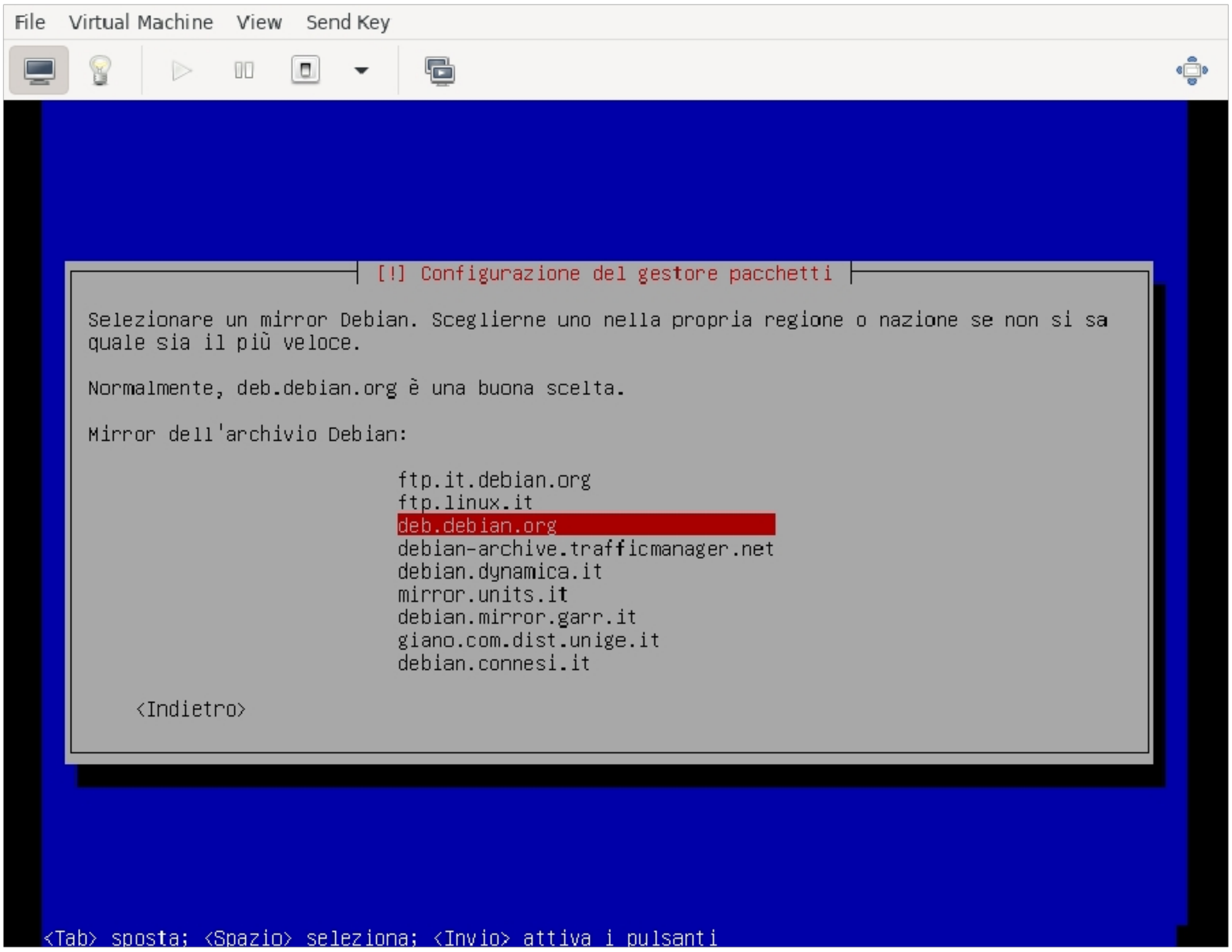


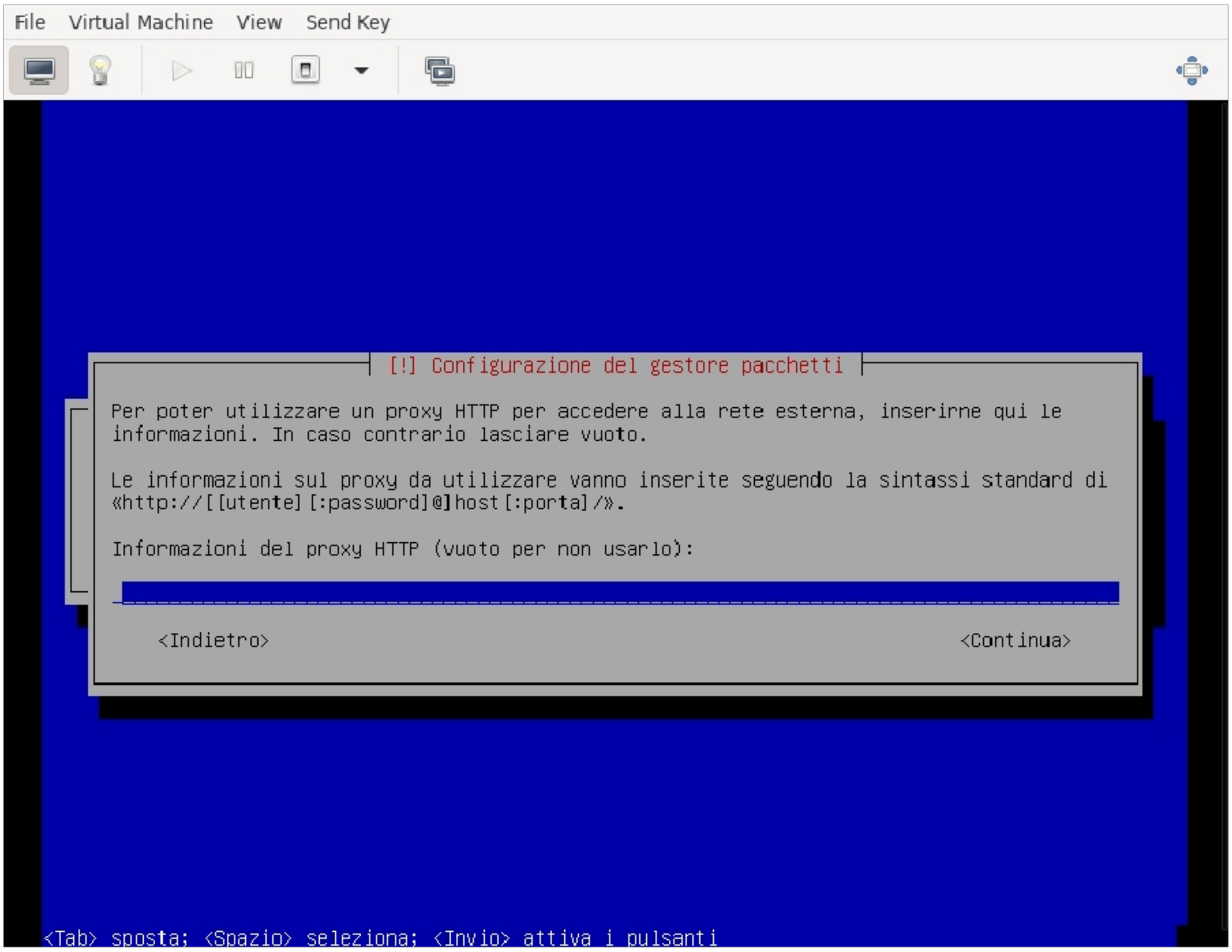
Once partitioning is complete and the base system installation is finished you will be asked whether to add additional CDs or DVDs, answer No:



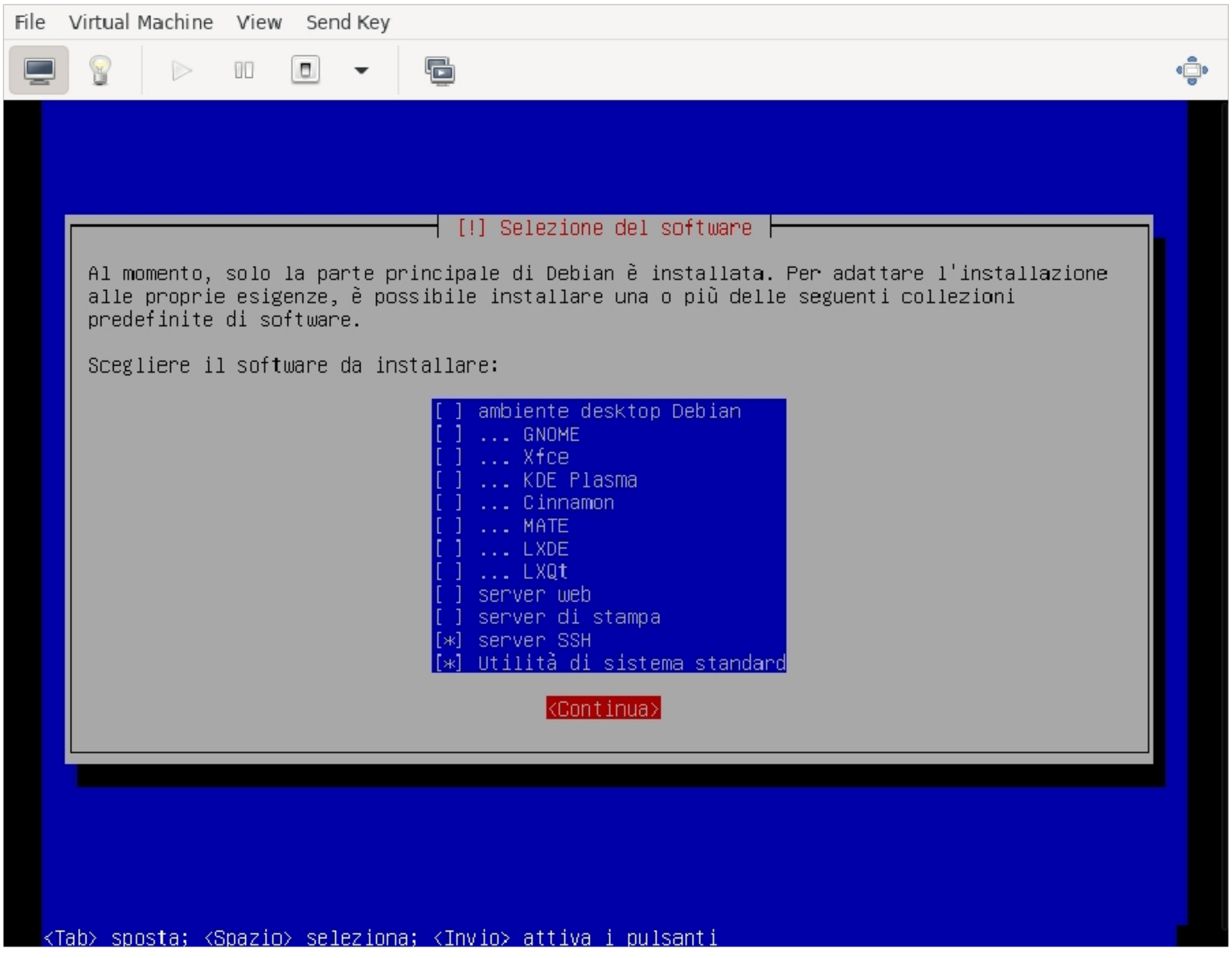
so when asked to configure package repositories, use the closest mirror, it will not be necessary, being over the WAN, to use a proxy.


File Virtual Machine View Send Key
[!] Configurazione del gestore pacchetti
Lo scopo è quello di trovare un mirror dell'archivio Debian che sia vicino alla propria rete. Attenzione perché le nazioni vicine o anche la propria non sono sempre le scelte migliori.
Nazione del mirror dell'archivio Debian:
Cechia
Cile
Cina
Corea del sud
Costa Rica
Croazia
Danimarca
El Salvador
Estonia
Filippine
Finlandia
Francia
Georgia
Germania
Giappone
Grecia
Hong Kong
India
Indonesia
Iran
Israele
Italia
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

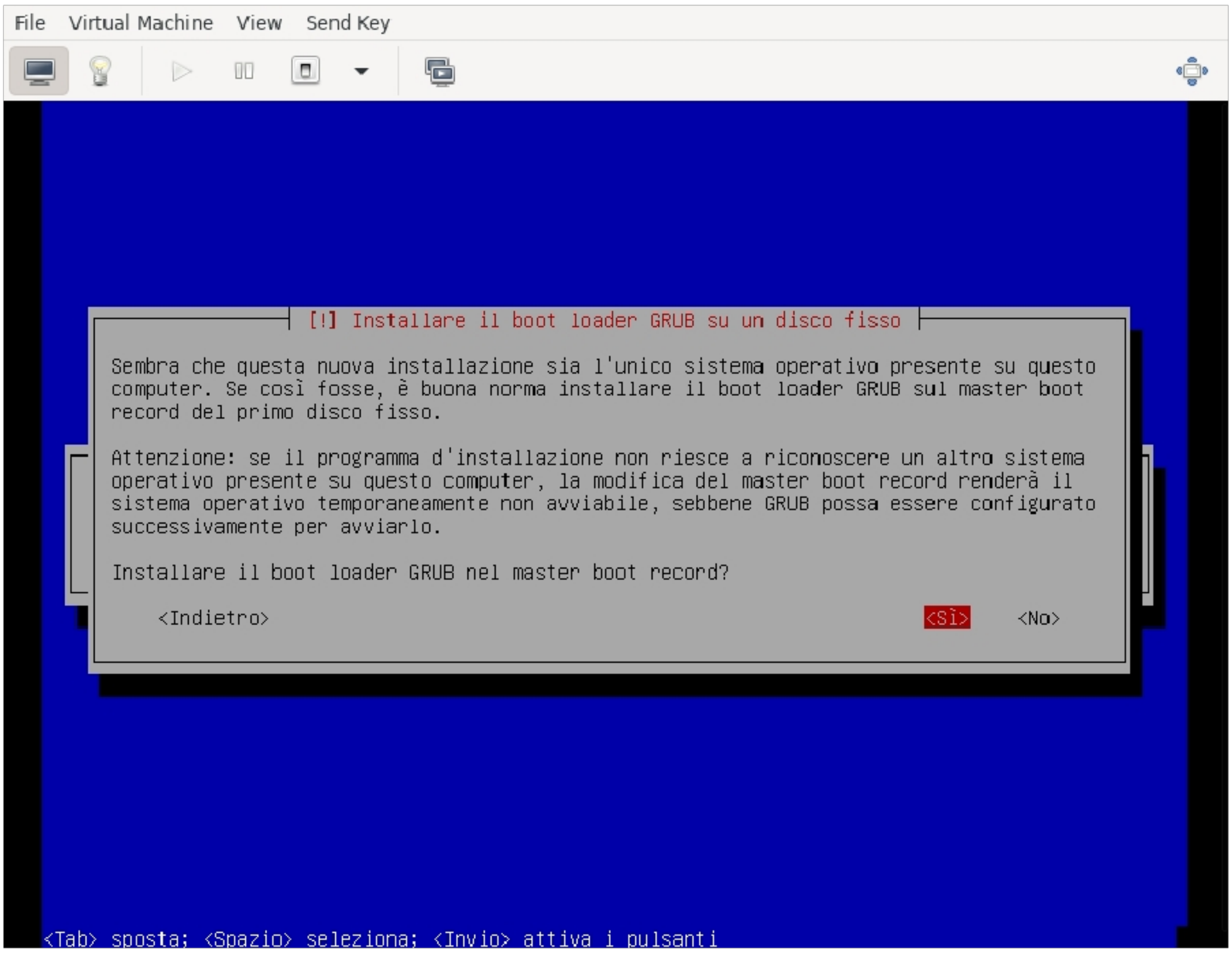

File Virtual Machine View Send Key
[!] Configurazione del gestore pacchetti
Selezionare un mirror Debian. Sceglierne uno nella propria regione o nazione se non si sa quale sia il più veloce.
Normalmente, deb.debian.org è una buona scelta.
Mirror dell'archivio Debian:
ftp.it.debian.org
ftp.linux.it
deb.debian.org
debian-archive.trafficmanager.net
debian.dynamica.it
mirror.units.it
debian.mirror.garr.it
giano.com.dist.unige.it
debian.connesi.it
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

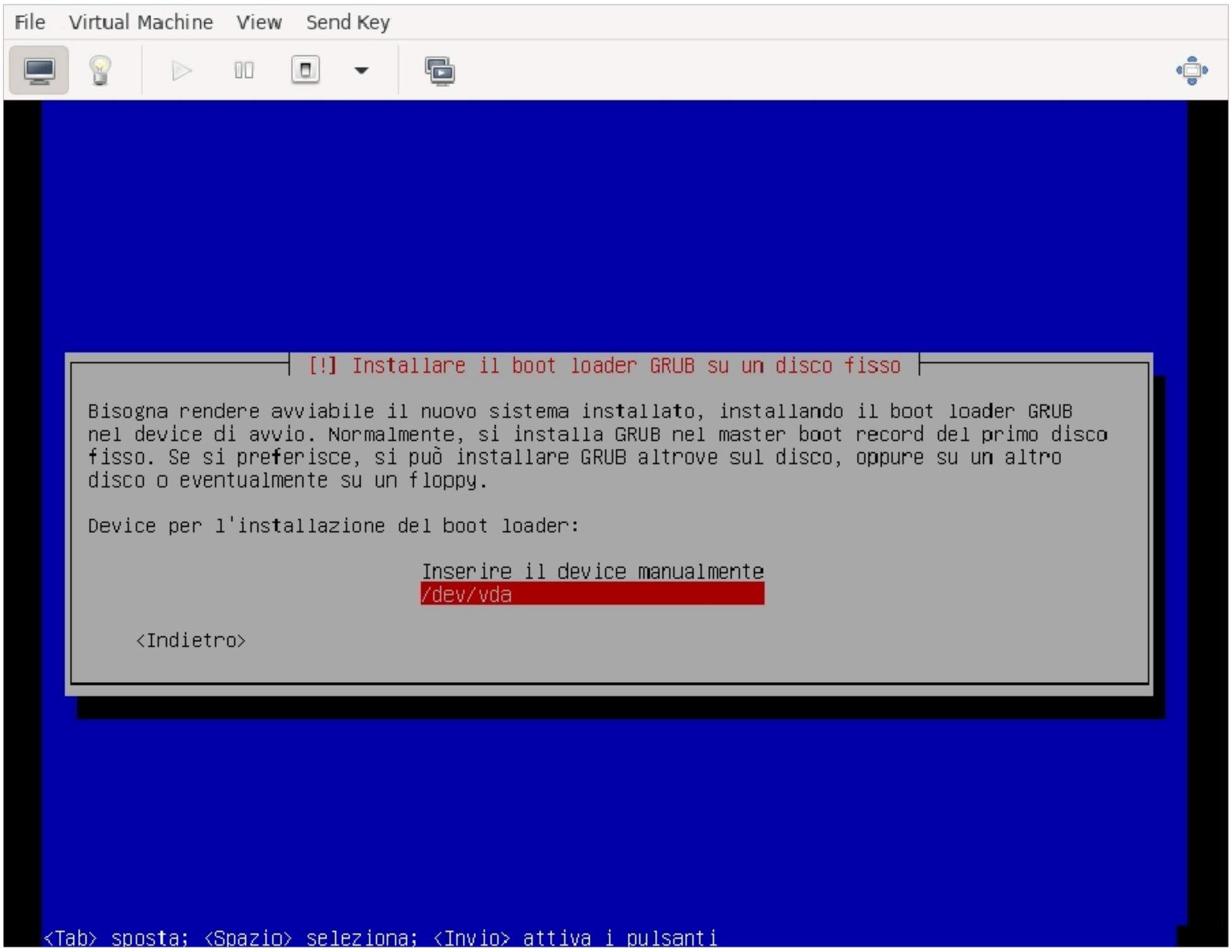


Respond as you prefer to the request to participate or not to participate in the popularity contest survey, and in the software selection choose only the items "SSH server" and "standard system utilities."



and complete the installation with GRUB installed on the disk's Master Boot Record:


File Virtual Machine View Send Key
[!] Installare il boot loader GRUB su un disco fisso
Sembra che questa nuova installazione sia l'unico sistema operativo presente su questo computer. Se così fosse, è buona norma installare il boot loader GRUB sul master boot record del primo disco fisso.
Attenzione: se il programma d'installazione non riesce a riconoscere un altro sistema operativo presente su questo computer, la modifica del master boot record renderà il sistema operativo temporaneamente non avviabile, sebbene GRUB possa essere configurato successivamente per avviarlo.
Installare il boot loader GRUB nel master boot record?
<Indietro>
<Sì>
<No>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti



When the installation is complete, restart the server, possibly removing the installation CD and restoring the boot order to boot.

Post-installation configurations

Once the Debian installation is complete, you need to finalize the initial machine configurations before you can launch `fuss-server create`. The first step is to configure the second network interface for the LAN; you will have to edit `/etc/network/interfaces` to add the relevant configuration with something like:

```
# lan
allow-hotplug enp2s0
iface enp2s0 inet static
      address 192.168.0.1
      netmask 255.255.255.0
      192.168.0.0 network
```

and activate the interface with `ifup enp2s0`.

You will then need to configure the software sources for the packages, adding lines for the backports repository and the FUSS repository in `/etc/apt/sources.list`:

```
deb http://deb.debian.org/debian/ bookworm-backports main
deb [signed-by=/usr/share/keyrings/fuss-keyring.gpg] http://archive.fuss.bz.it/ ␣
↪bookworm main
```

finally you will have to import the GPG key from the FUSS repository with:

```
# apt install gnupg
# wget -qO /usr/share/keyrings/fuss-keyring.gpg https://archive.fuss.bz.it/apt.gpg
# apt update
```

at this point you will be able to install the fuss-server package:

```
# apt install fuss-server
```

Once the initial configuration of the machine is complete, you can continue with the configuration of the fuss-server as already explained in the *Server Configuration* section.

1.4 Traditional installation of FUSS Client

We now move on to the installation of the first client.

1.4.1 USB flash drive preparation

As a first step, you need to download the latest version of Debian 12 "bookworm" Xfce live ISO image by taking from https://cdimage.debian.org/mirror/cdimage/release/current-live/amd64/iso-hybrid/ the file `debian-live-<version>amd64-xfce.iso`

You need a USB flash drive with a minimum size of at least 4 GB to which the downloaded ISO image is to be copied. As also mentioned above, in GNU/Linux you can use the `dd` command. After inserting the flash drive into the PC where the image is available, check with the `lsscsi` command which device has been assigned to the flash drive. In the example we use `/dev/sdX` where X can be any of the letters `a`, `b`, `c`, etc. Assuming the downloaded ISO is for amd64 architecture, as root, give the command

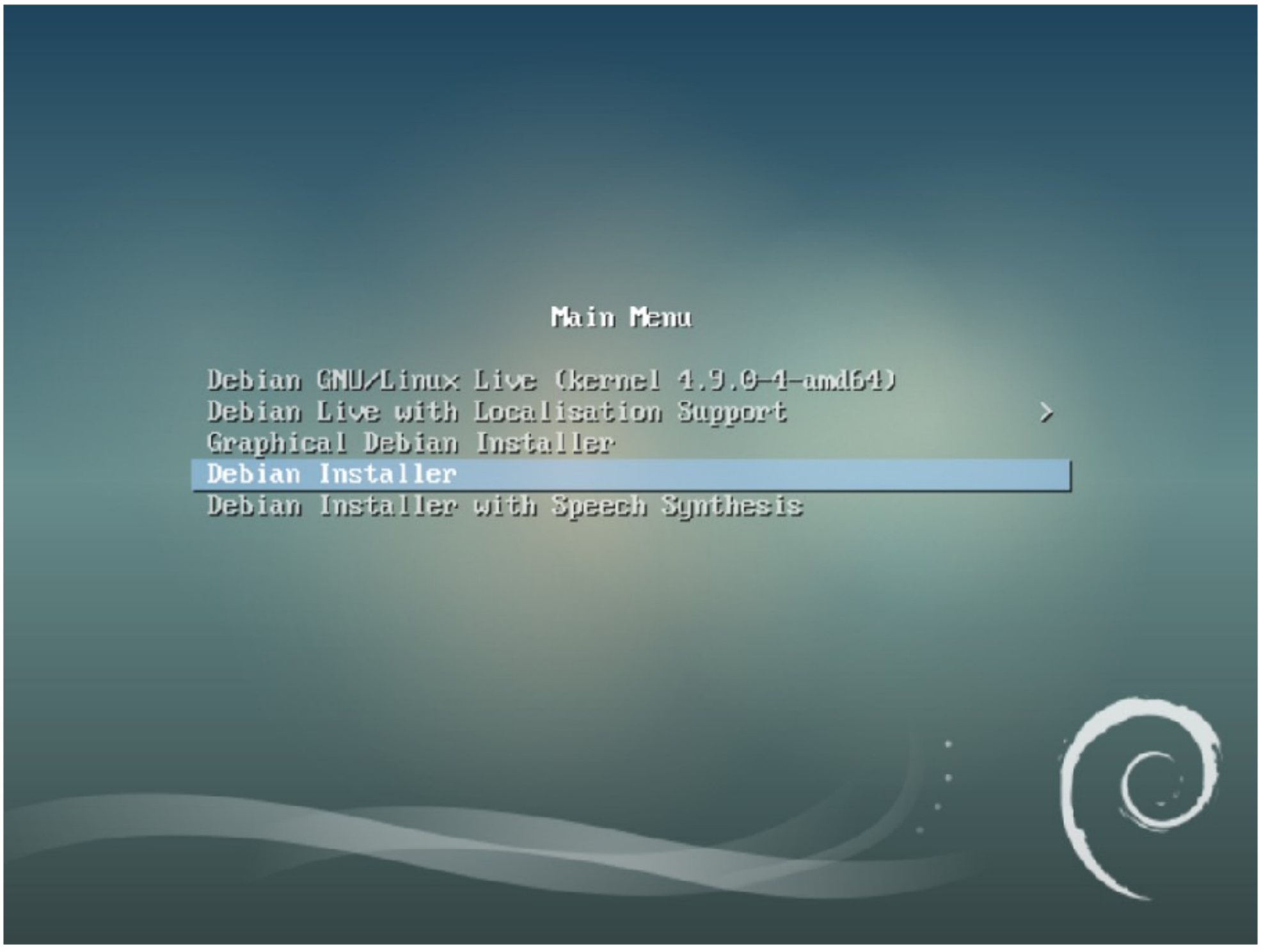
```
dd if=/PERCORSO_IMMAGINE/debian-live-<version>-amd64-xfce.iso of=/dev/sdX bs=4M␣
↪status=progress
```

Having prepared the USB flash drive, insert it into the PC/notebook and after starting it, be sure to choose the flash drive itself as the boot device.

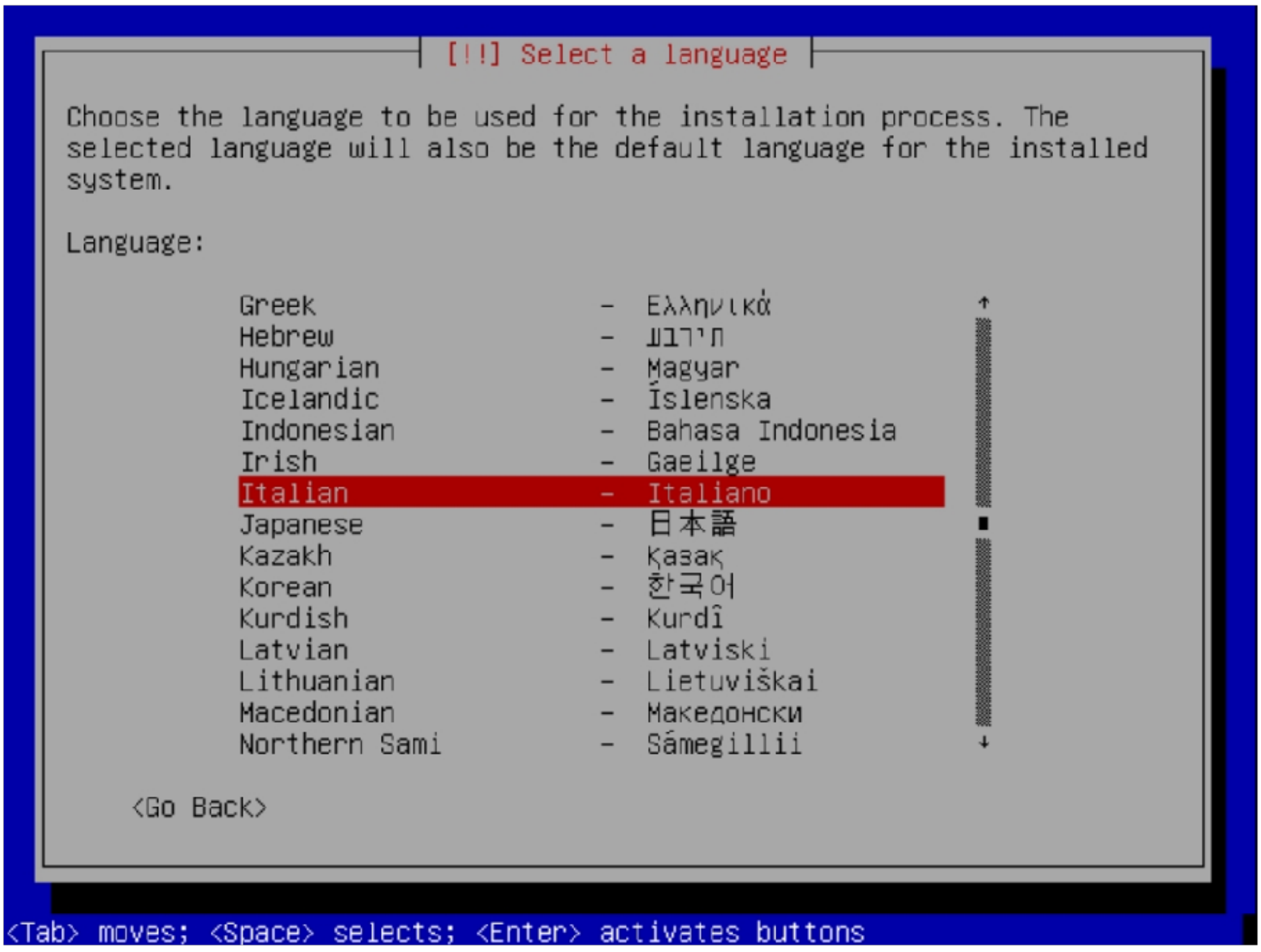
1.4.2 Installation wizard

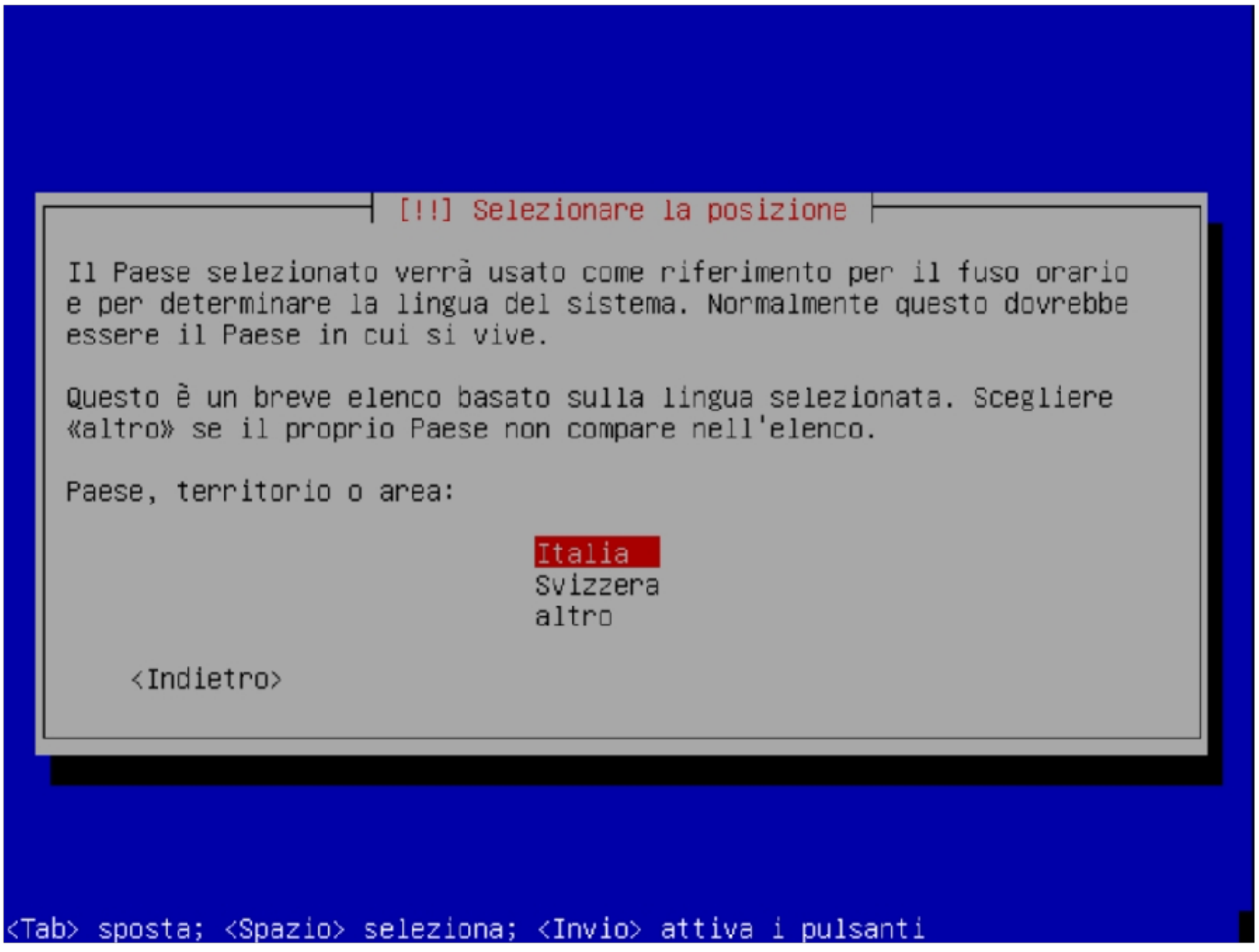
For images, the installation procedure for the first client is shown below. The console installer (Debian Installer) was chosen. Alternatively, you can opt for the graphical installer (Graphical Debian Installer).

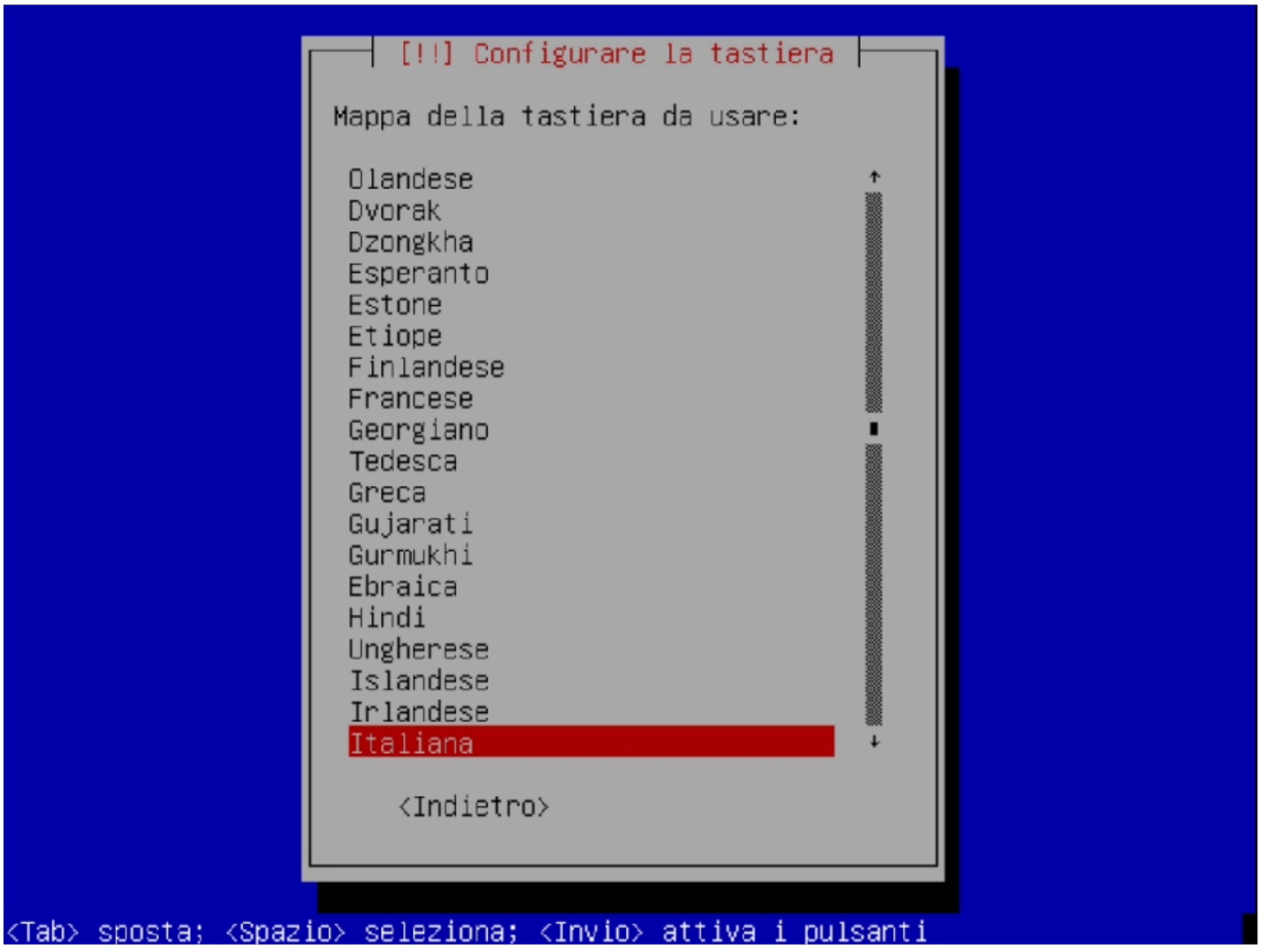
Note: If you want to use FUSS in *LIVE* mode, choose the first option. The default user credentials are `user - live`.



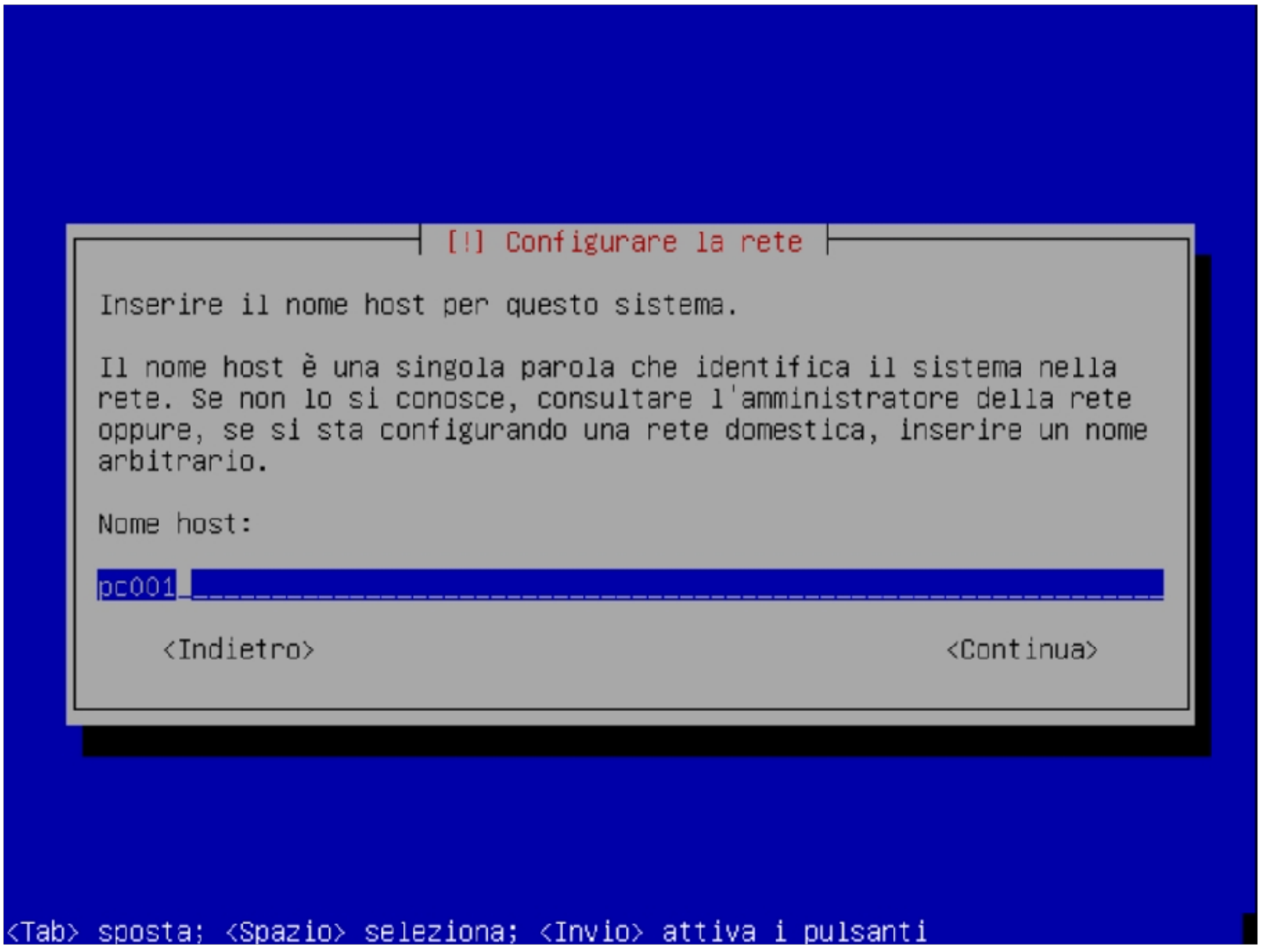
Choice of language and keyboard.


[!!] 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:
Greek - Ελληνικά
Hebrew - עברית
Hungarian - Magyar
Icelandic - Íslenska
Indonesian - Bahasa Indonesia
Irish - Gaeilge
Italian - Italiano
Japanese - 日本語
Kazakh - Қазақ
Korean - 한국어
Kurdish - Kurdî
Latvian - Latviski
Lithuanian - Lietuviškai
Macedonian - Македонски
Northern Sami - Sámegillii
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

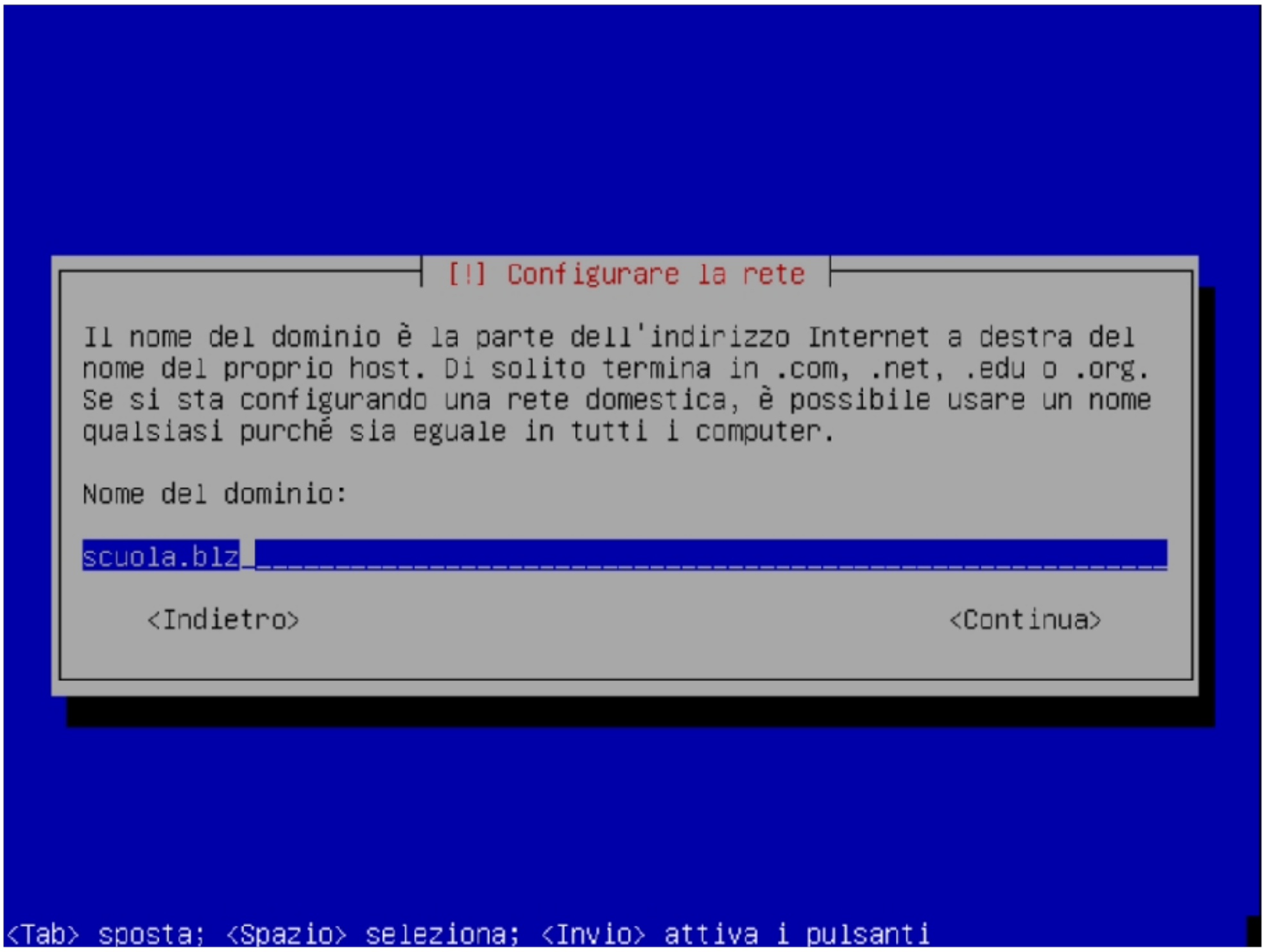

[!!] Selezionare la posizione
Il Paese selezionato verrà usato come riferimento per il fuso orario e per determinare la lingua del sistema. Normalmente questo dovrebbe essere il Paese in cui si vive.
Questo è un breve elenco basato sulla lingua selezionata. Scegliere «altro» se il proprio Paese non compare nell'elenco.
Paese, territorio o area:
Italia
Svizzera
altro
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti



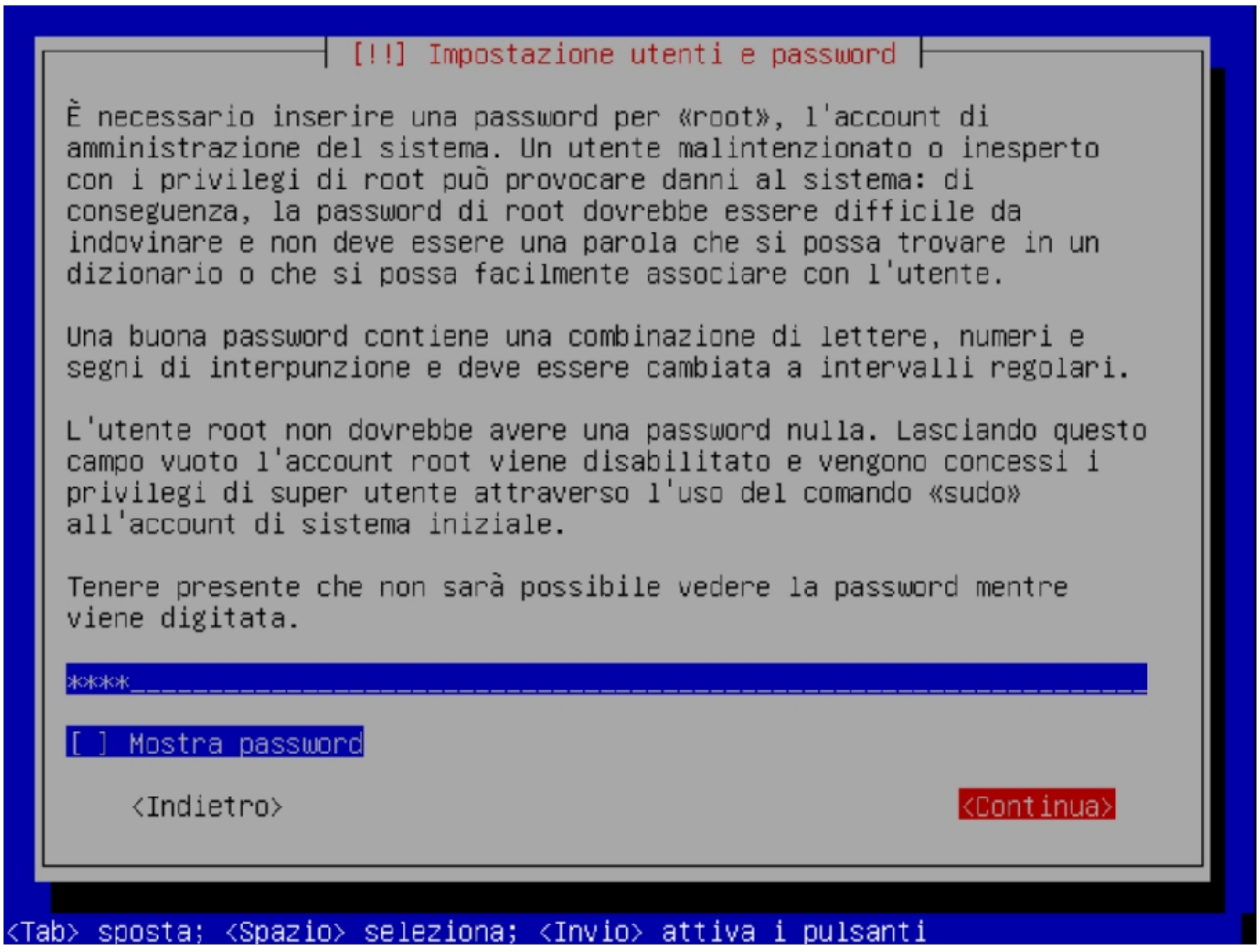
Enter the name of the host.

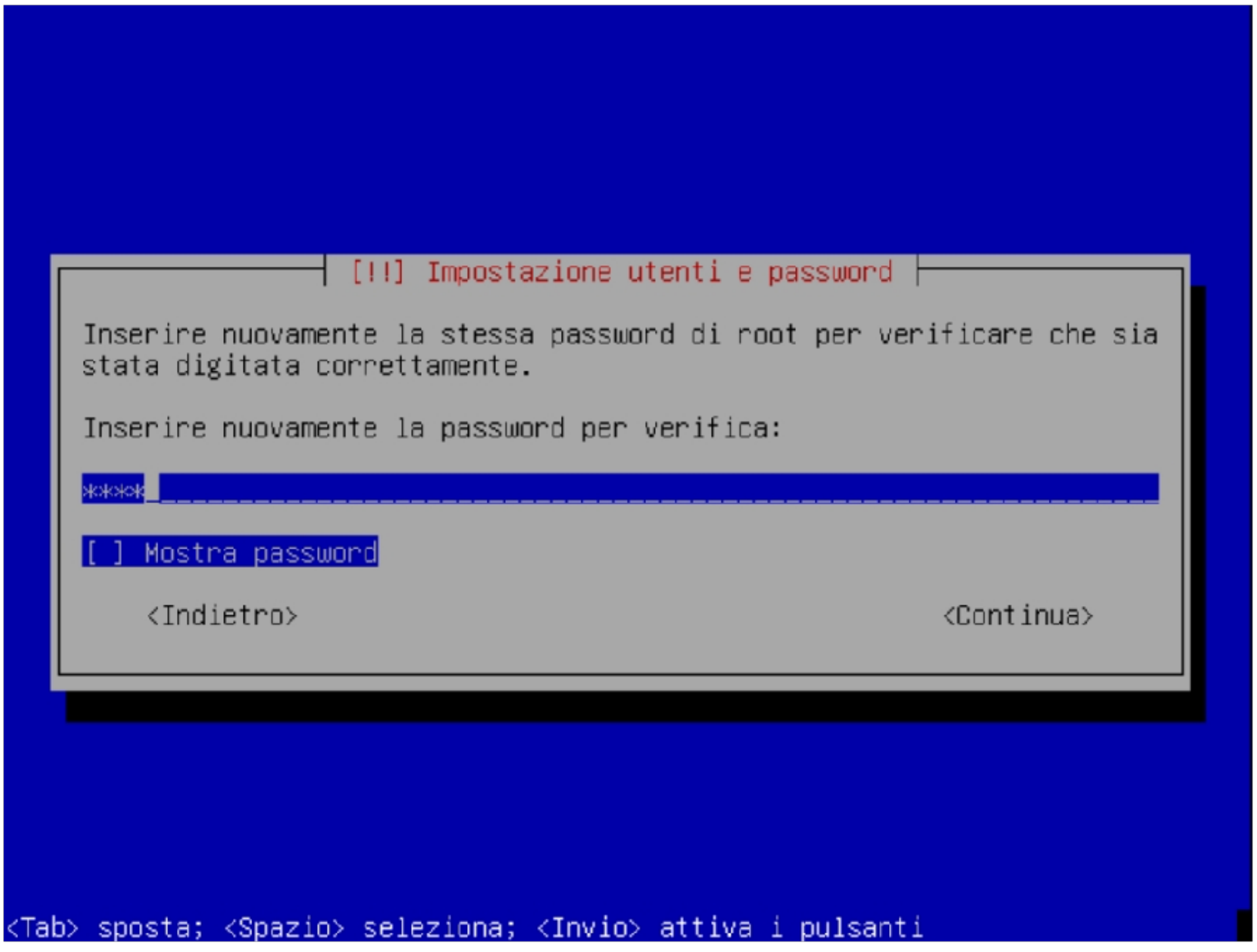


The internal domain in which the host is located, as defined during server installation.

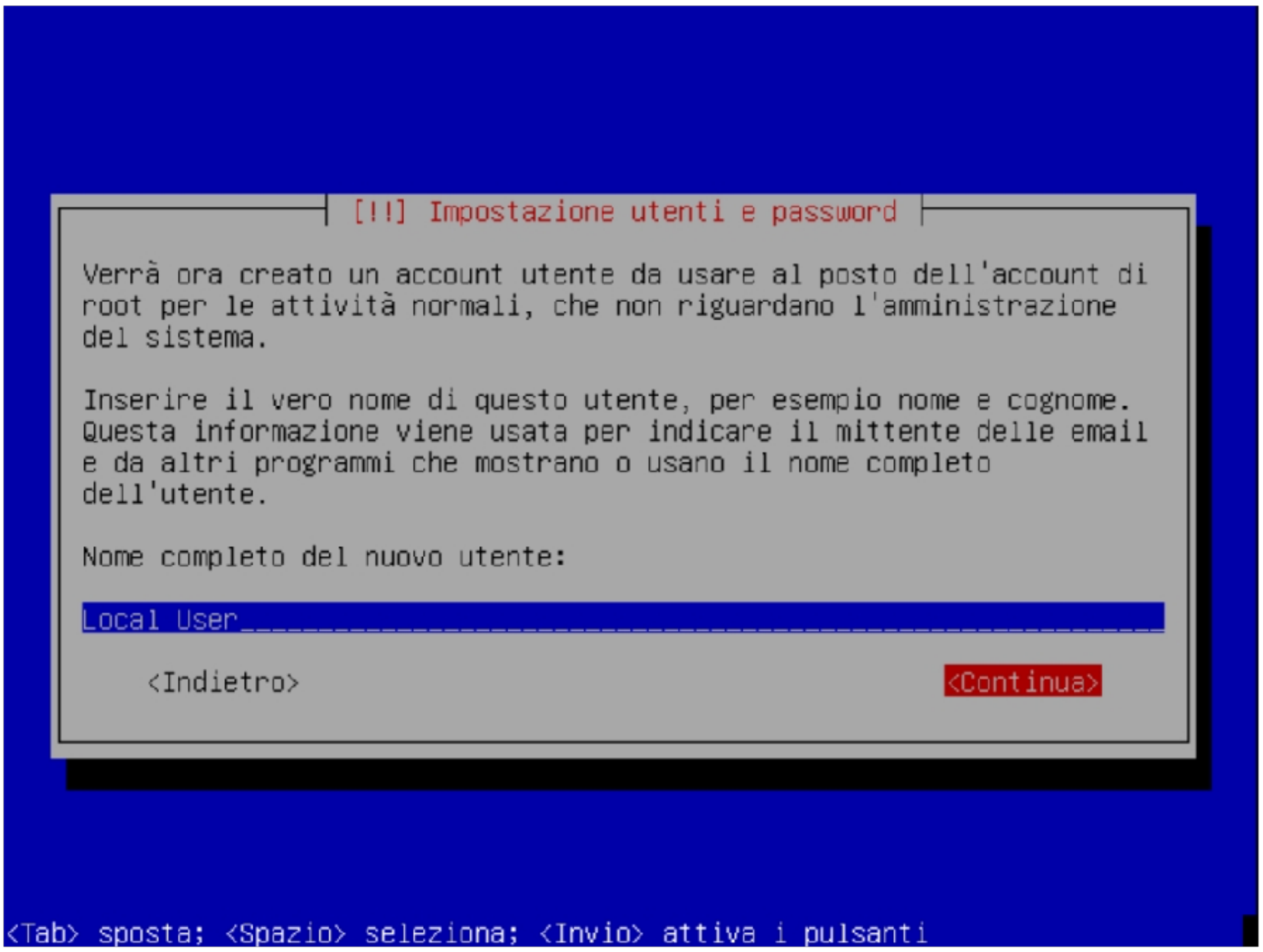


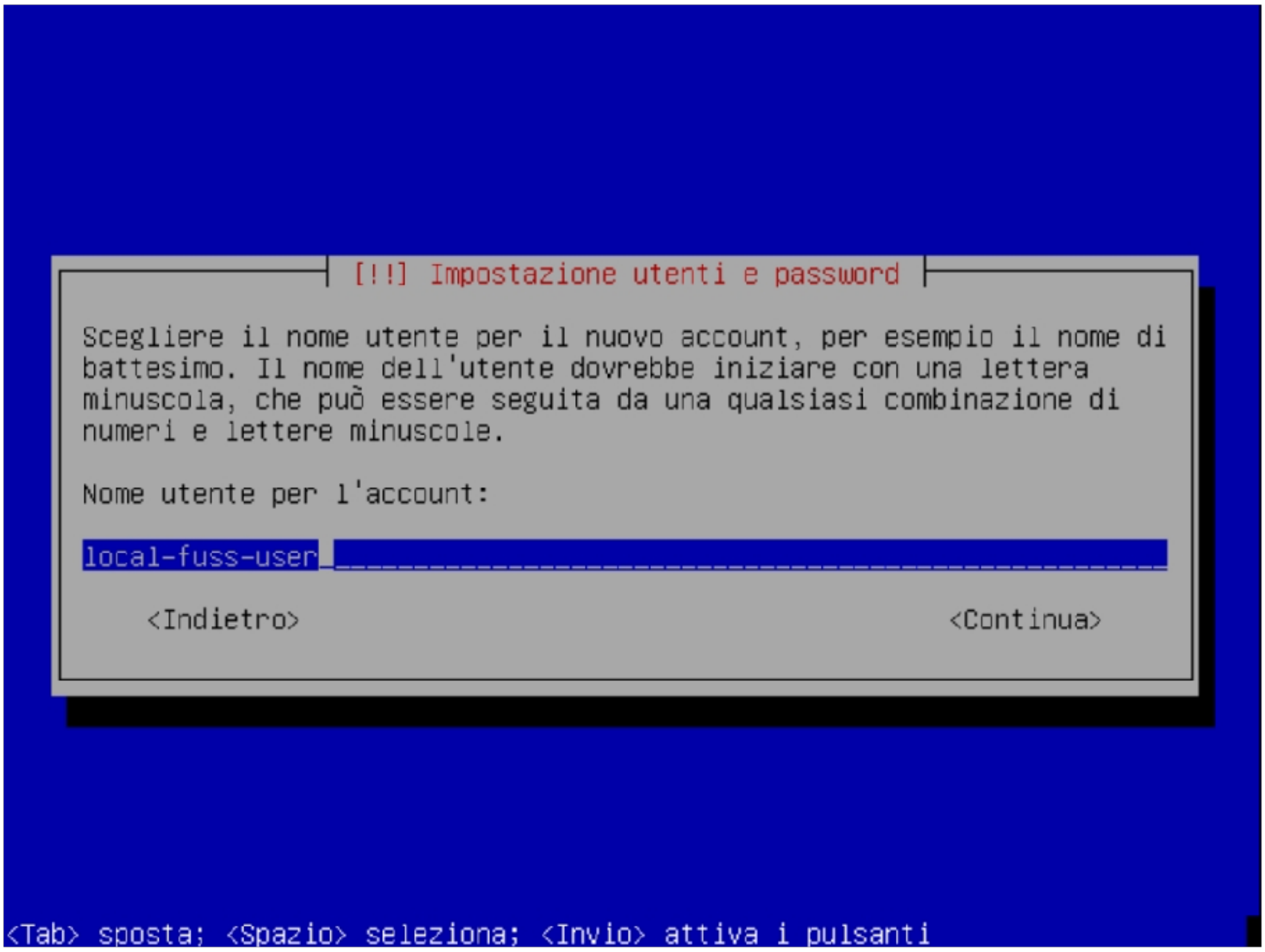
Setting the root password.

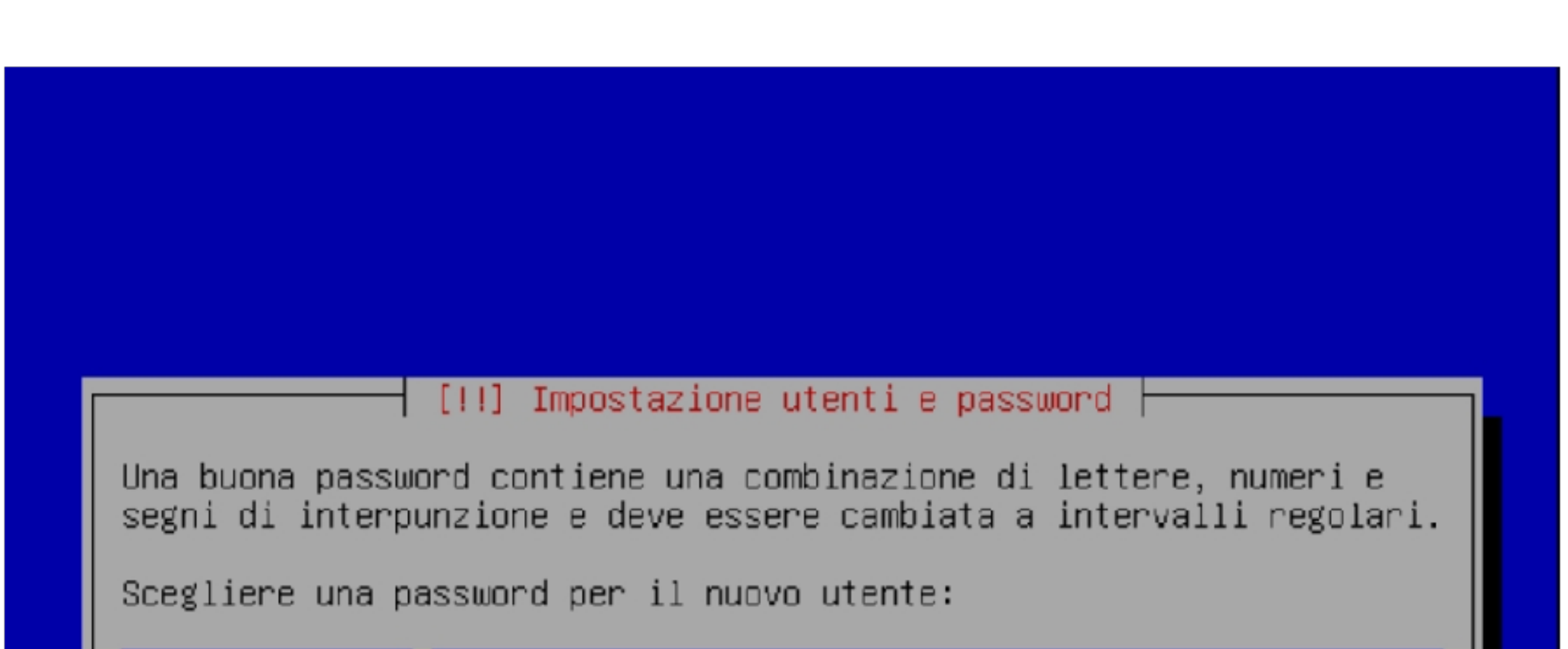

[!!] Impostazione utenti e password
È necessario inserire una password per «root», l'account di amministrazione del sistema. Un utente malintenzionato o inesperto con i privilegi di root può provocare danni al sistema: di conseguenza, la password di root dovrebbe essere difficile da indovinare e non deve essere una parola che si possa trovare in un dizionario o che si possa facilmente associare con l'utente.
Una buona password contiene una combinazione di lettere, numeri e segni di interpunzione e deve essere cambiata a intervalli regolari.
L'utente root non dovrebbe avere una password nulla. Lasciando questo campo vuoto l'account root viene disabilitato e vengono concessi i privilegi di super utente attraverso l'uso del comando «sudo» all'account di sistema iniziale.
Tenere presente che non sarà possibile vedere la password mentre viene digitata.
****
[ ] Mostra password
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

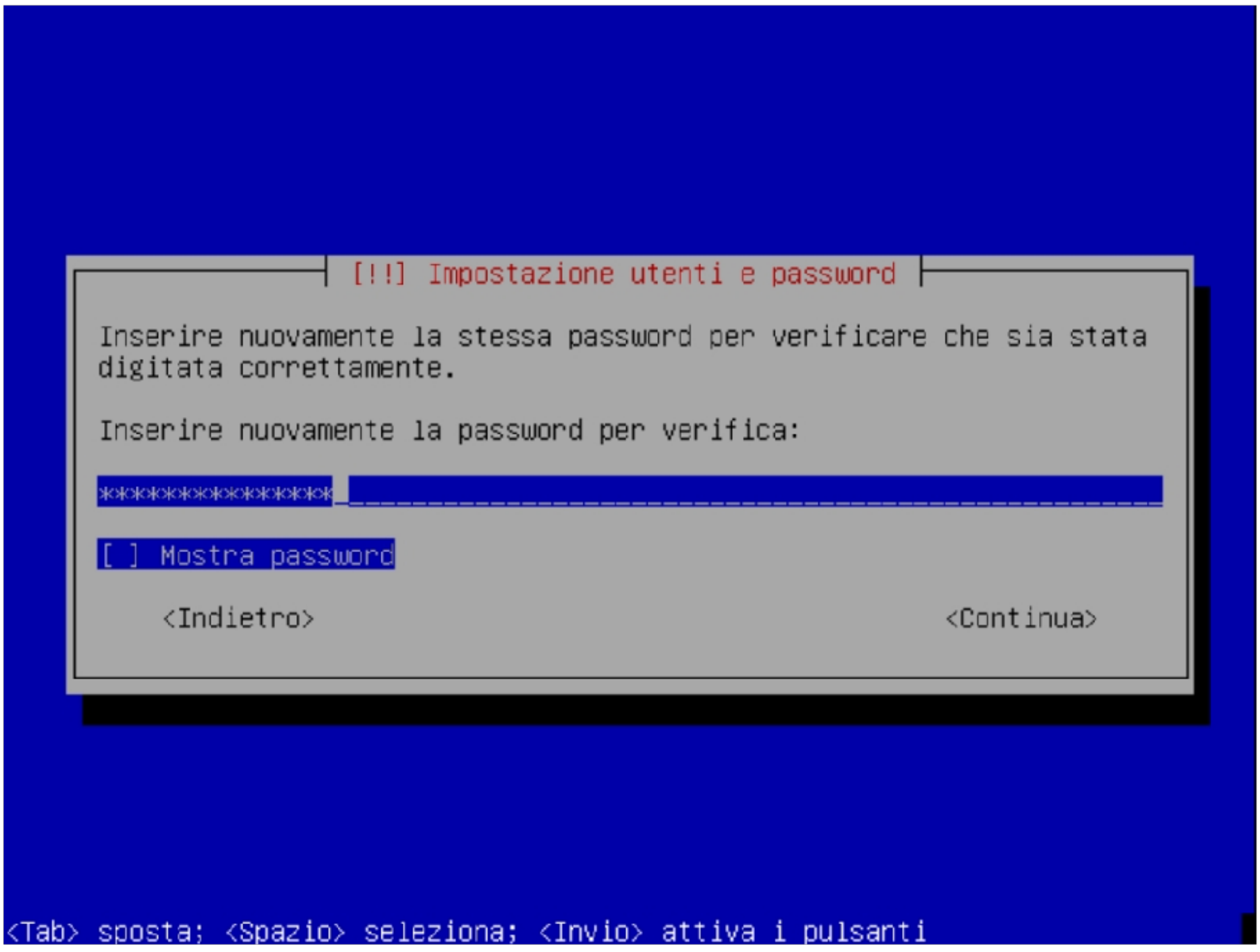

[!!] Impostazione utenti e password
Inserire nuovamente la stessa password di root per verificare che sia stata digitata correttamente.
Inserire nuovamente la password per verifica:
****
[ ] Mostra password
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

Creating a local user.

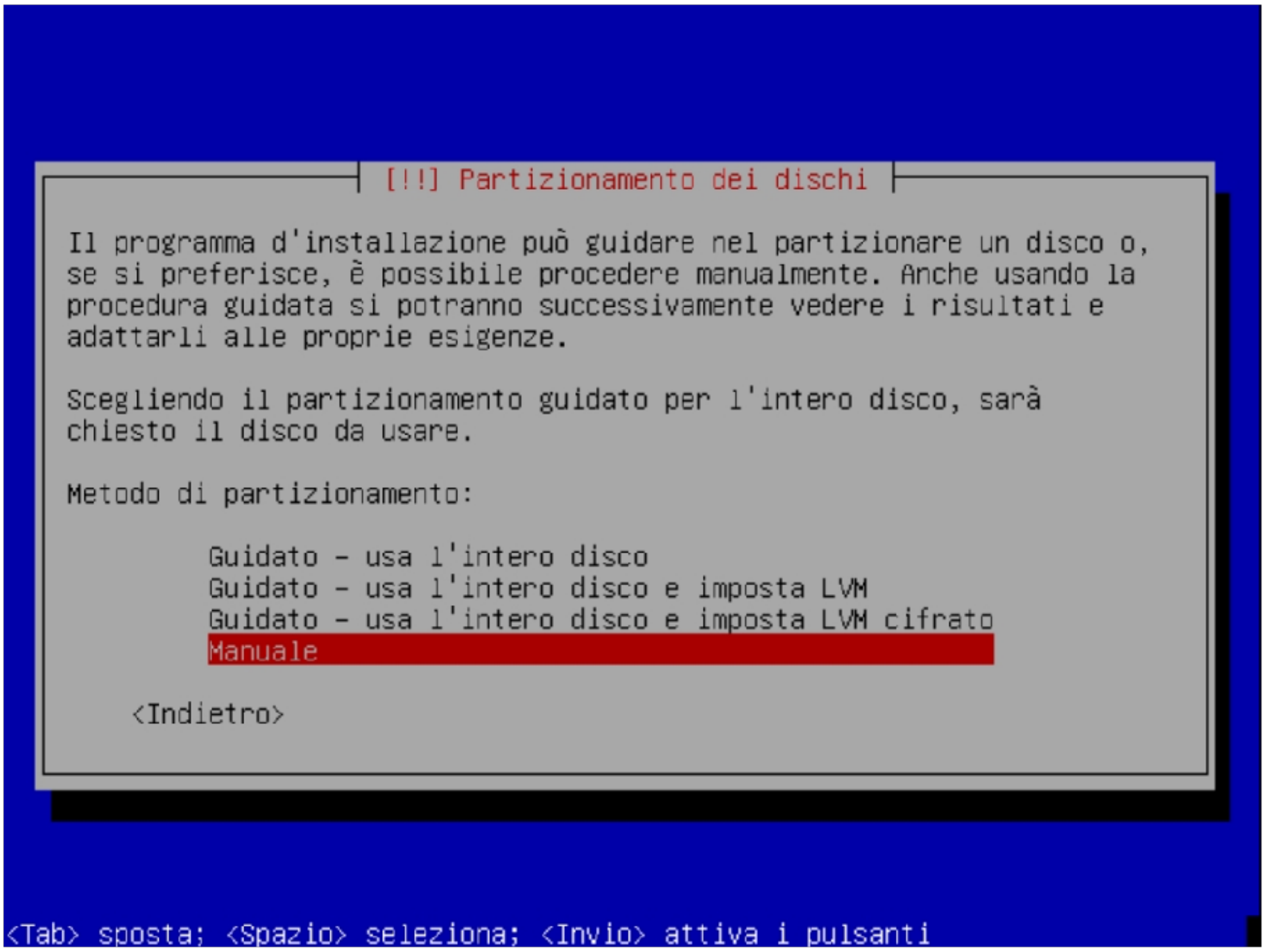


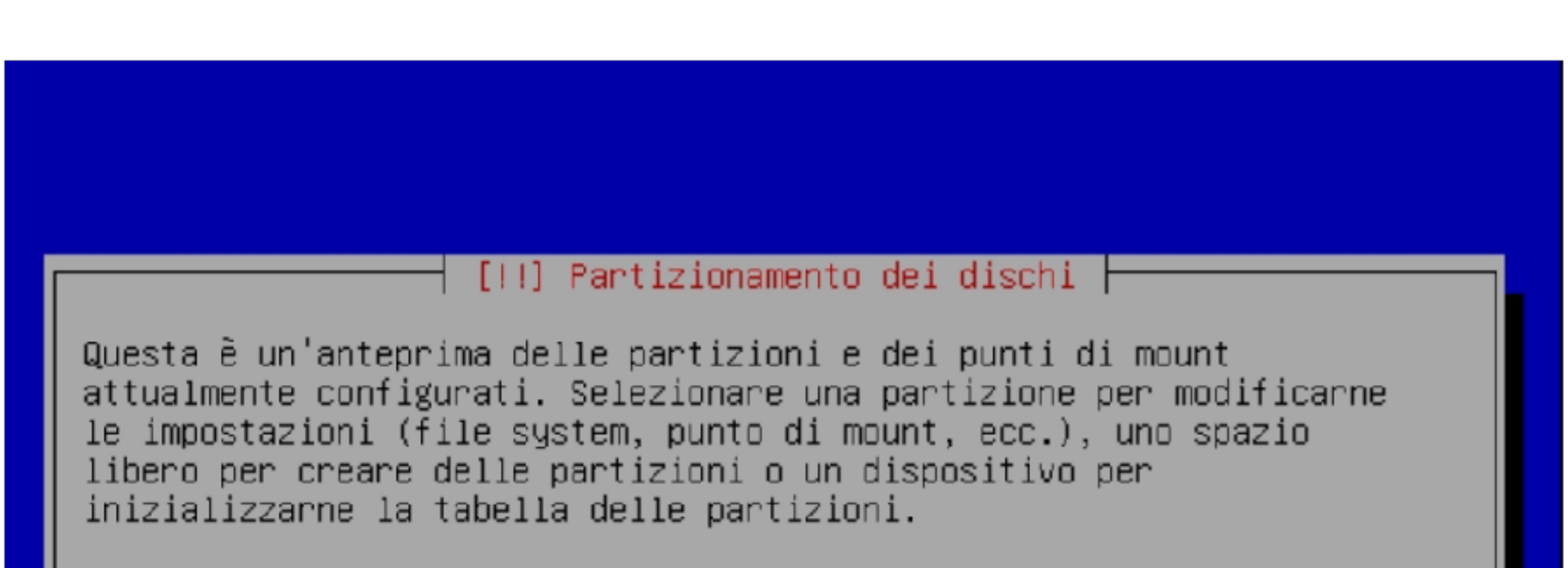

[!!] Impostazione utenti e password
Scegliere il nome utente per il nuovo account, per esempio il nome di battesimo. Il nome dell'utente dovrebbe iniziare con una lettera minuscola, che può essere seguita da una qualsiasi combinazione di numeri e lettere minuscole.
Nome utente per l'account:
local-fuss-user
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

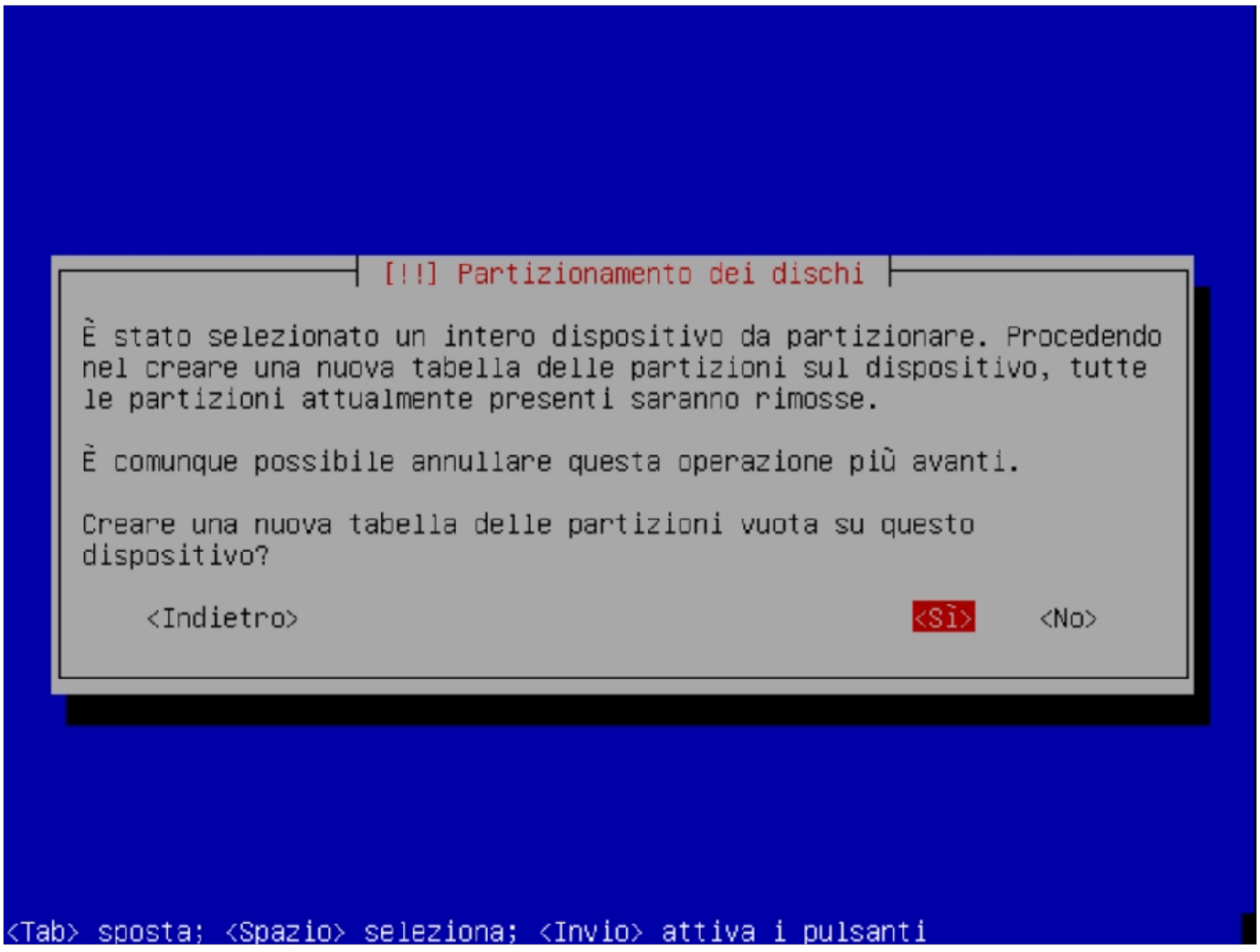

[!!] Impostazione utenti e password
Una buona password contiene una combinazione di lettere, numeri e segni di interpunzione e deve essere cambiata a intervalli regolari.
Scegliere una password per il nuovo utente:
[ ] Mostra password
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

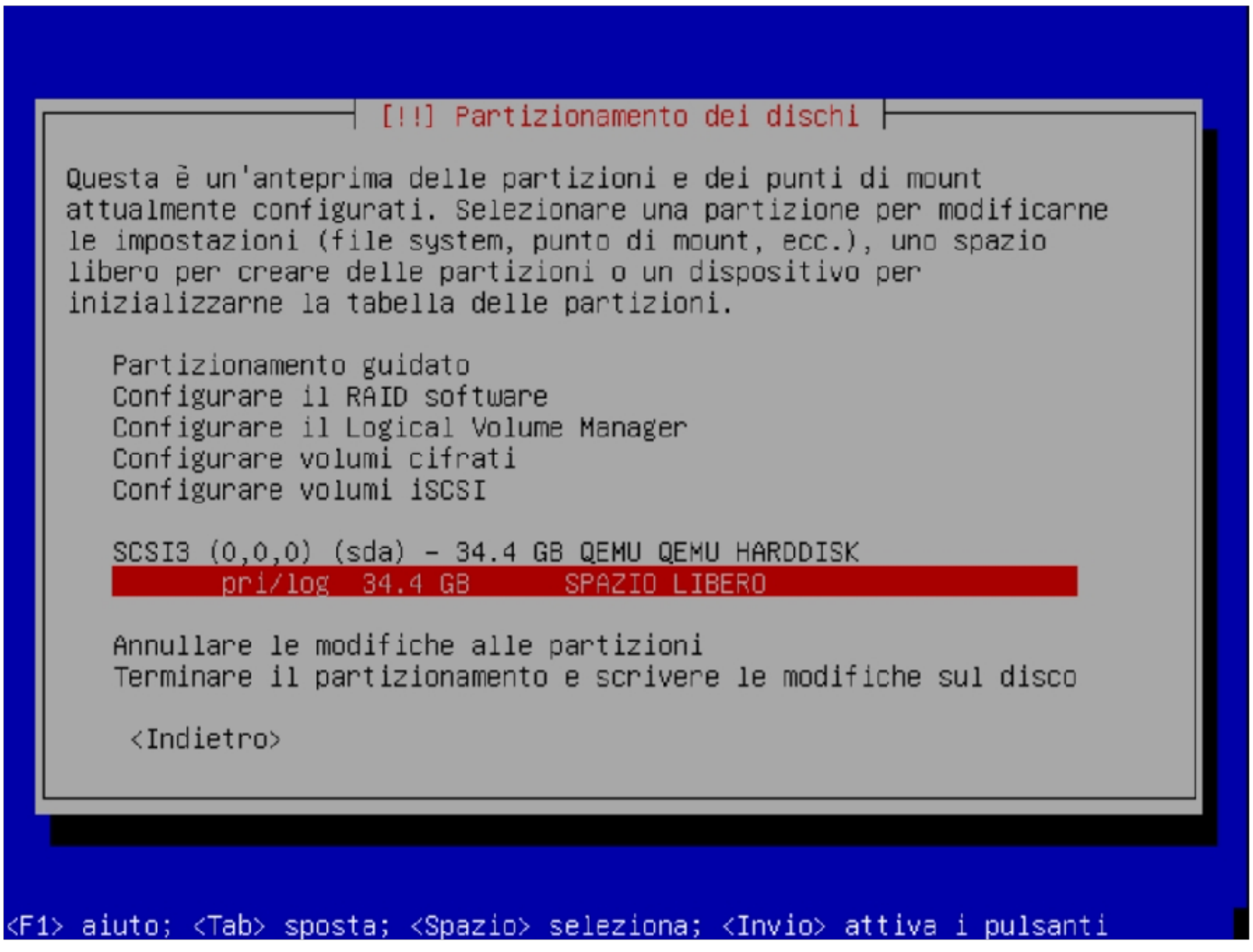


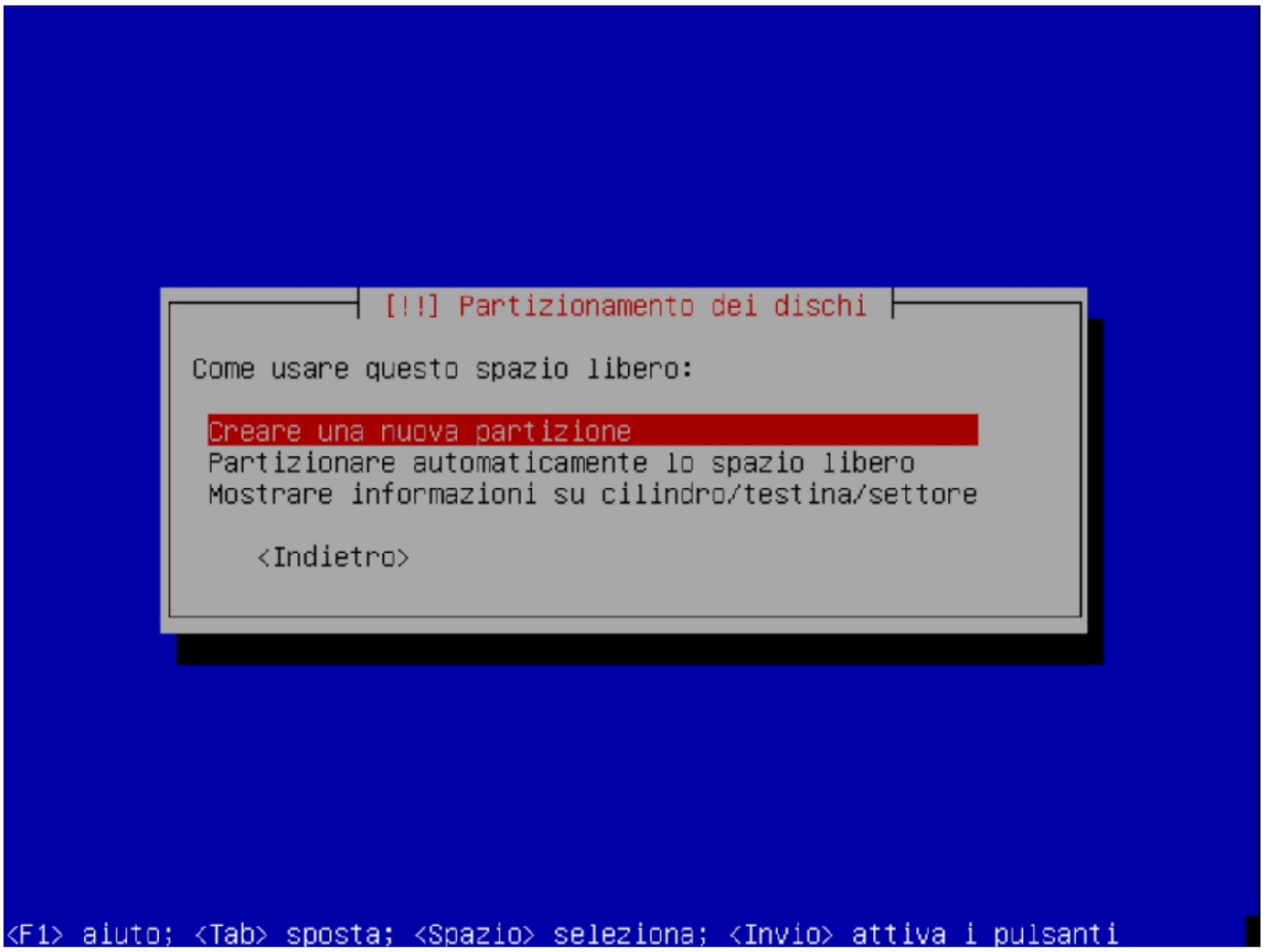
Disk partitioning. Choose manual partitioning by setting up a swap partition and one for the root (/ or root) filesystem.

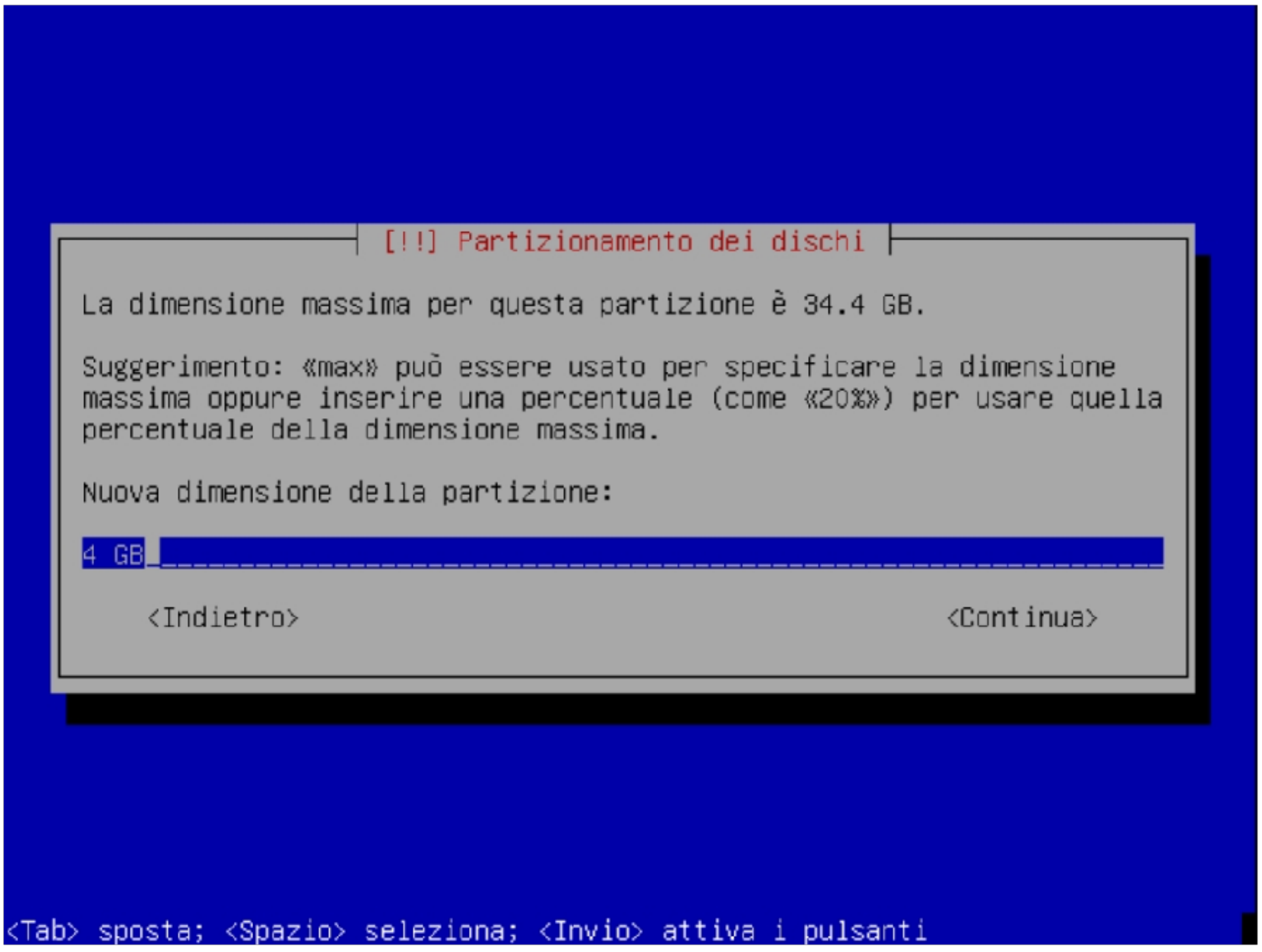

[!!] Partizionamento dei dischi
Il programma d'installazione può guidare nel partizionare un disco o, se si preferisce, è possibile procedere manualmente. Anche usando la procedura guidata si potranno successivamente vedere i risultati e adattarli alle proprie esigenze.
Scegliendo il partizionamento guidato per l'intero disco, sarà chiesto il disco da usare.
Metodo di partizionamento:
Guidato - usa l'intero disco
Guidato - usa l'intero disco e imposta LVM
Guidato - usa l'intero disco e imposta LVM cifrato
Manuale
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

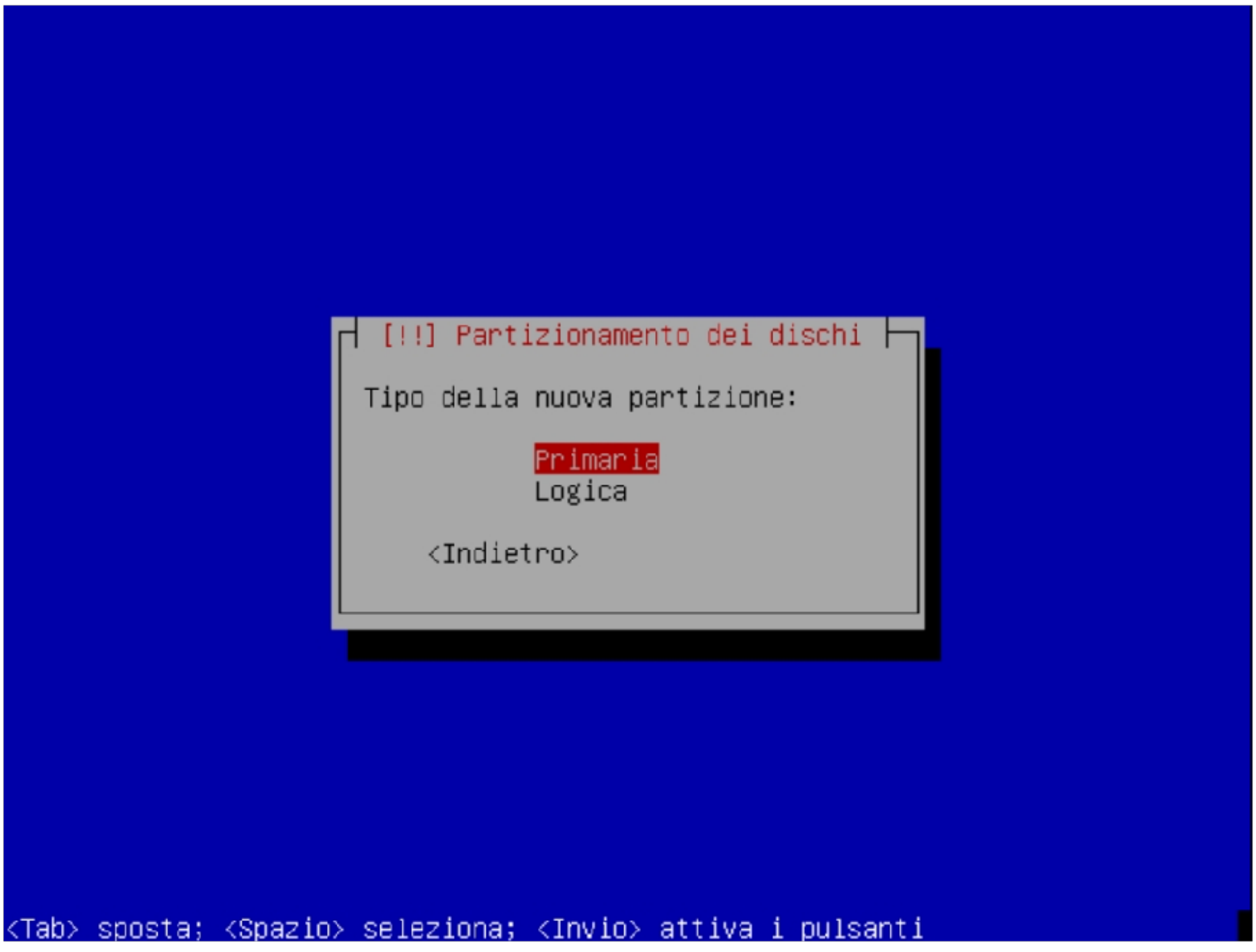

[!!] Partizionamento dei dischi
Questa è un'anteprima delle partizioni e dei punti di mount attualmente configurati. Selezionare una partizione per modificarne le impostazioni (file system, punto di mount, ecc.), uno spazio libero per creare delle partizioni o un dispositivo per inizializzarne la tabella delle partizioni.
Partizionamento guidato
Configurare volumi iSCSI
SCSI3 (0,0,0) (sda) - 34.4 GB QEMU QEMU HARDDISK
Annullare le modifiche alle partizioni
Terminare il partizionamento e scrivere le modifiche sul disco
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

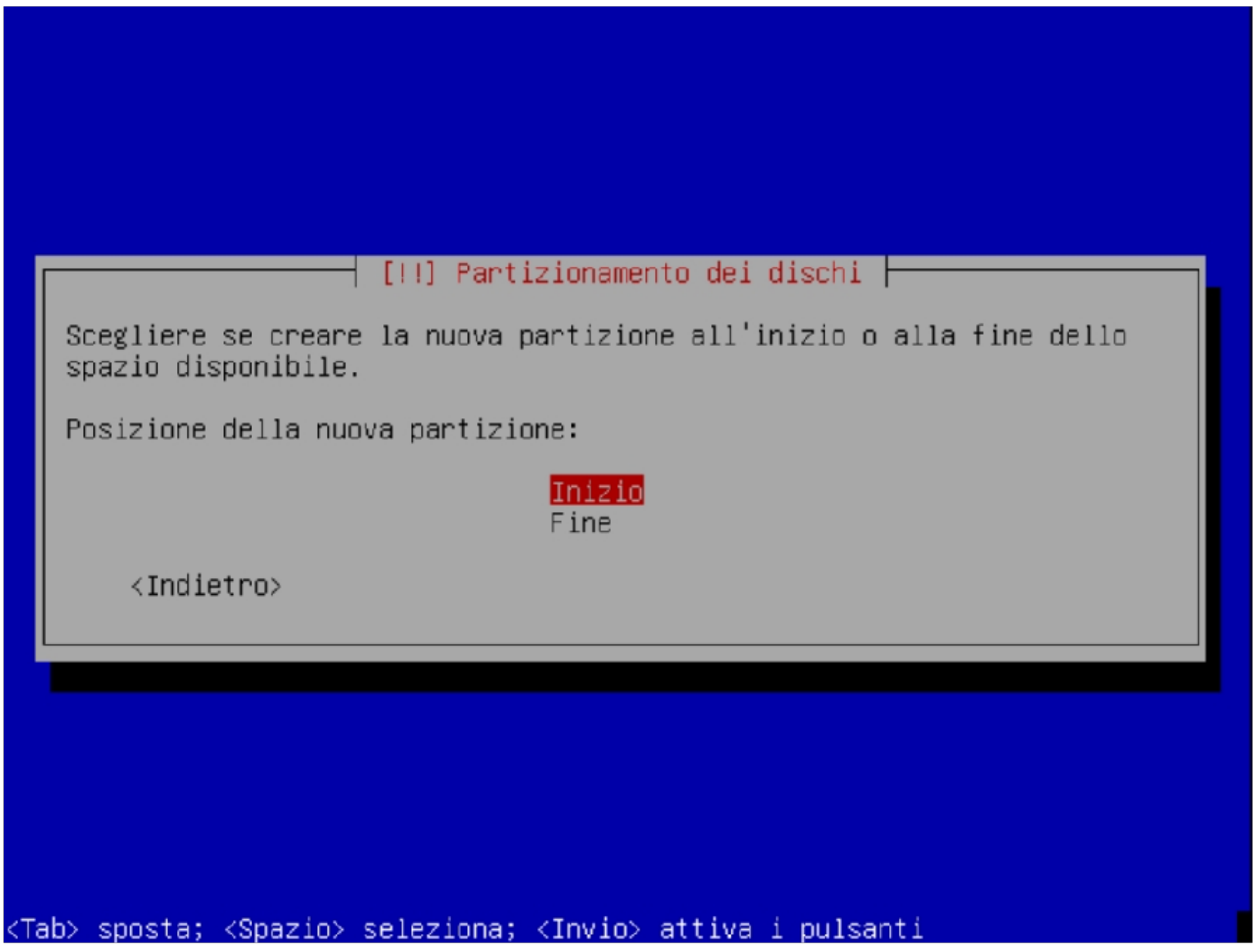

[!!] Partizionamento dei dischi
È stato selezionato un intero dispositivo da partizionare. Procedendo nel creare una nuova tabella delle partizioni sul dispositivo, tutte le partizioni attualmente presenti saranno rimosse.
È comunque possibile annullare questa operazione più avanti.
Creare una nuova tabella delle partizioni vuota su questo dispositivo?
<Indietro>
<Sì>
<No>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

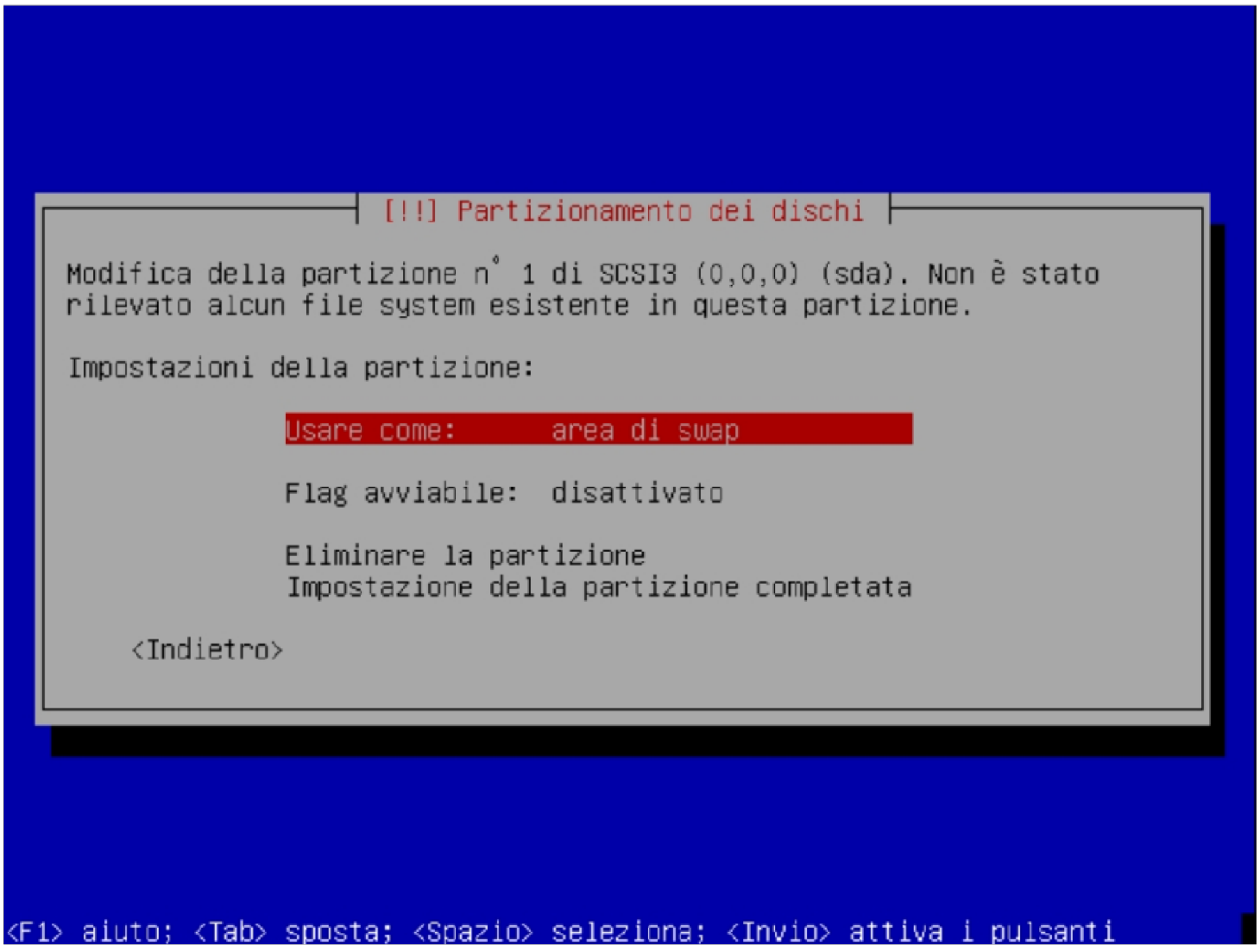

[!!] Partizionamento dei dischi
Questa è un'anteprima delle partizioni e dei punti di mount attualmente configurati. Selezionare una partizione per modificarne le impostazioni (file system, punto di mount, ecc.), uno spazio libero per creare delle partizioni o un dispositivo per inizializzarne la tabella delle partizioni.
Partizionamento guidato
Configurare il RAID software
Configurare il Logical Volume Manager
Configurare volumi cifrati
Configurare volumi iSCSI
SCSI3 (0,0,0) (sda) - 34.4 GB QEMU QEMU HARDDISK
pri/log 34.4 GB SPAZIO LIBERO
Annullare le modifiche alle partizioni
Terminare il partizionamento e scrivere le modifiche sul disco
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

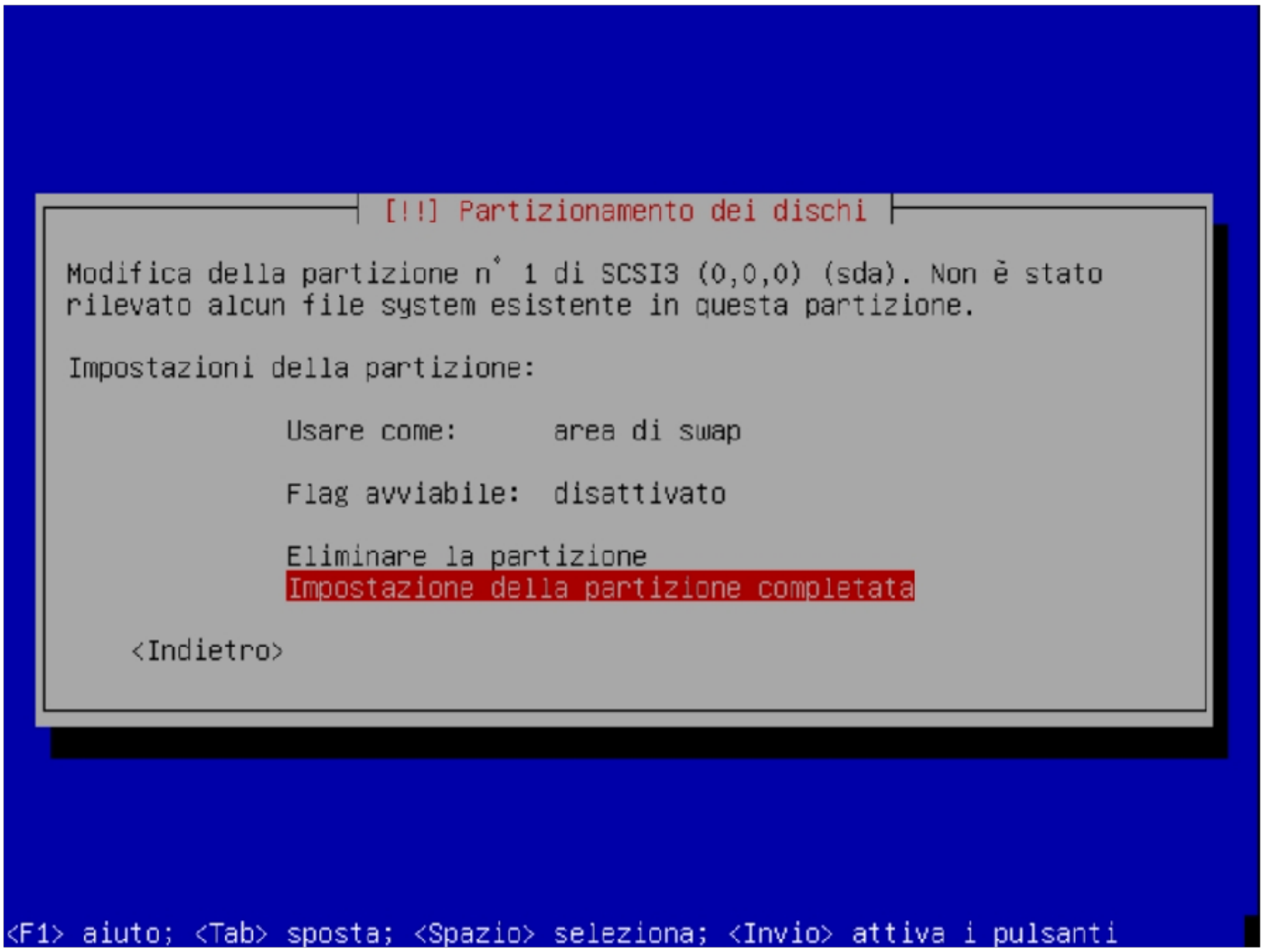

[!!] Partizionamento dei dischi
Come usare questo spazio libero:
Creare una nuova partizione
Partizionare automaticamente lo spazio libero
Mostrare informazioni su cilindro/testina/settore
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

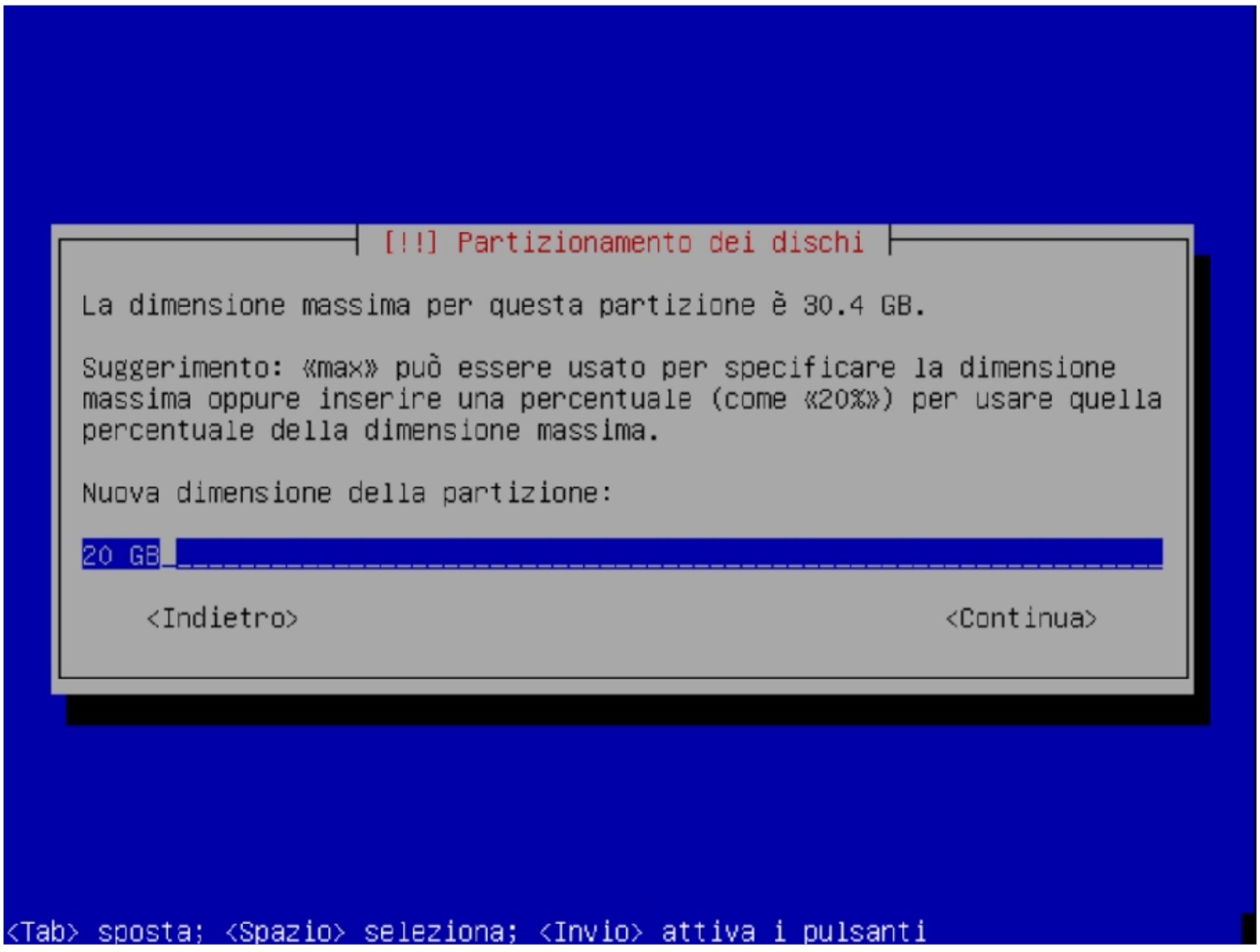

[!!] Partizionamento dei dischi
La dimensione massima per questa partizione è 34.4 GB.
Suggerimento: «max» può essere usato per specificare la dimensione massima oppure inserire una percentuale (come «20%») per usare quella percentuale della dimensione massima.
Nuova dimensione della partizione:
4 GB
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

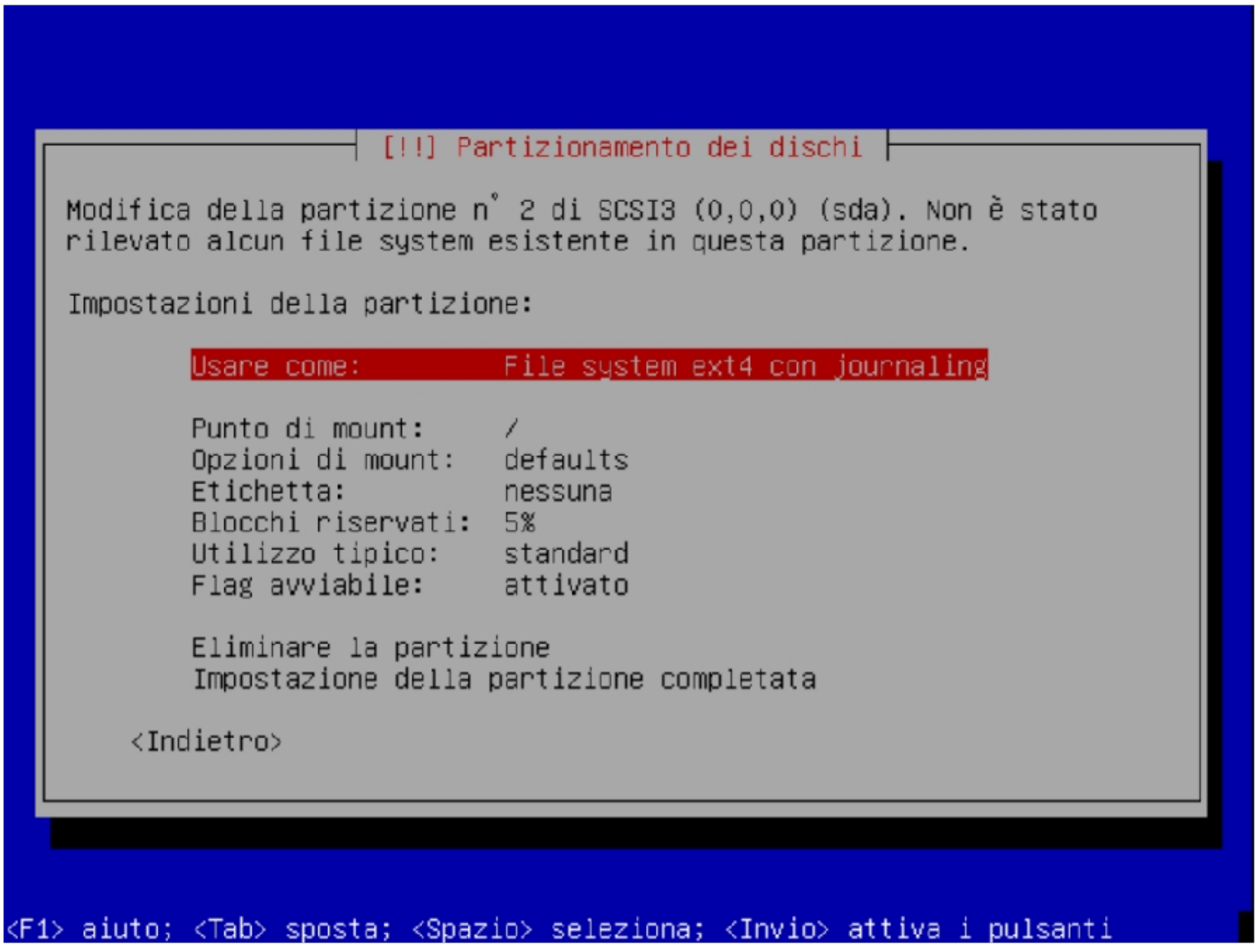

[!!] Partizionamento dei dischi
Tipo della nuova partizione:
Primaria
Logica
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

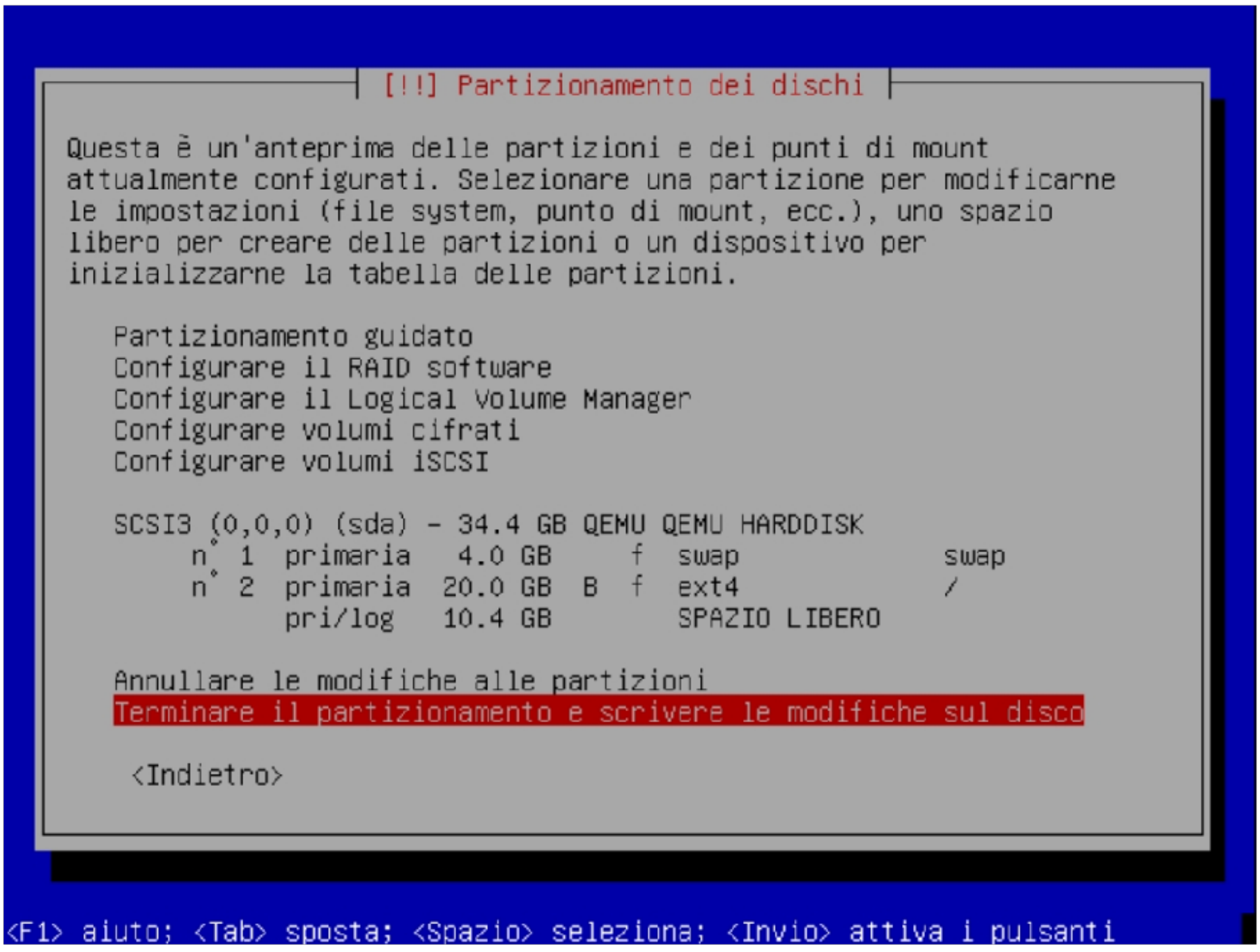

[!!] Partizionamento dei dischi
Scegliere se creare la nuova partizione all'inizio o alla fine dello spazio disponibile.
Posizione della nuova partizione:
Inizio
Fine
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti


[!!] Partizionamento dei dischi
Modifica della partizione n° 1 di SCSI3 (0,0,0) (sda). Non è stato rilevato alcun file system esistente in questa partizione.
Impostazioni della partizione:
Usare come: area di swap
Flag avviabile: disattivato
Eliminare la partizione
Impostazione della partizione completata
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

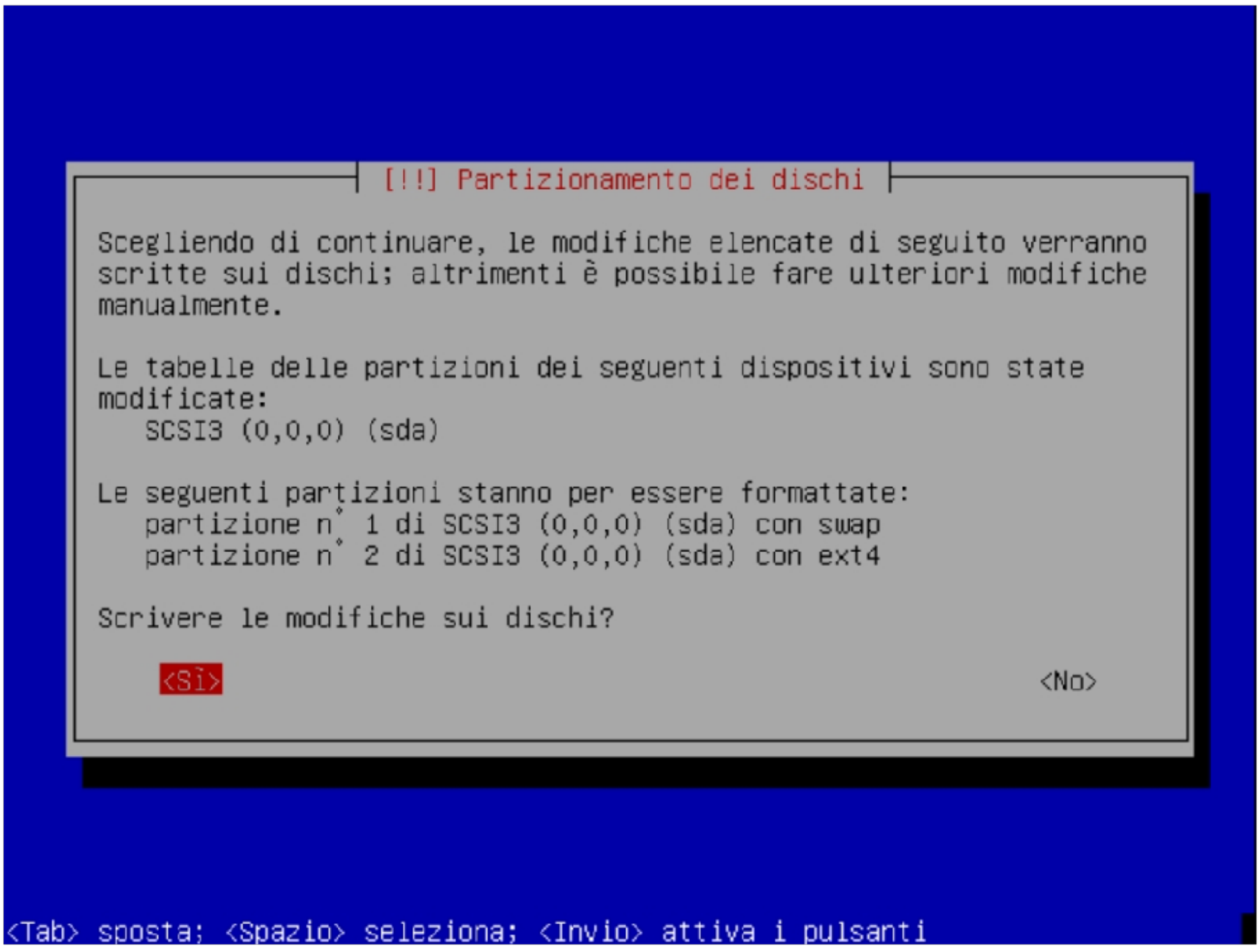

[!!] Partizionamento dei dischi
Modifica della partizione n° 1 di SCSI3 (0,0,0) (sda). Non è stato rilevato alcun file system esistente in questa partizione.
Impostazioni della partizione:
Usare come: area di swap
Flag avviabile: disattivato
Eliminare la partizione
Impostazione della partizione completata
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti


[!!] Partizionamento dei dischi
La dimensione massima per questa partizione è 30.4 GB.
Suggerimento: «max» può essere usato per specificare la dimensione massima oppure inserire una percentuale (come «20%») per usare quella percentuale della dimensione massima.
Nuova dimensione della partizione:
20 GB
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

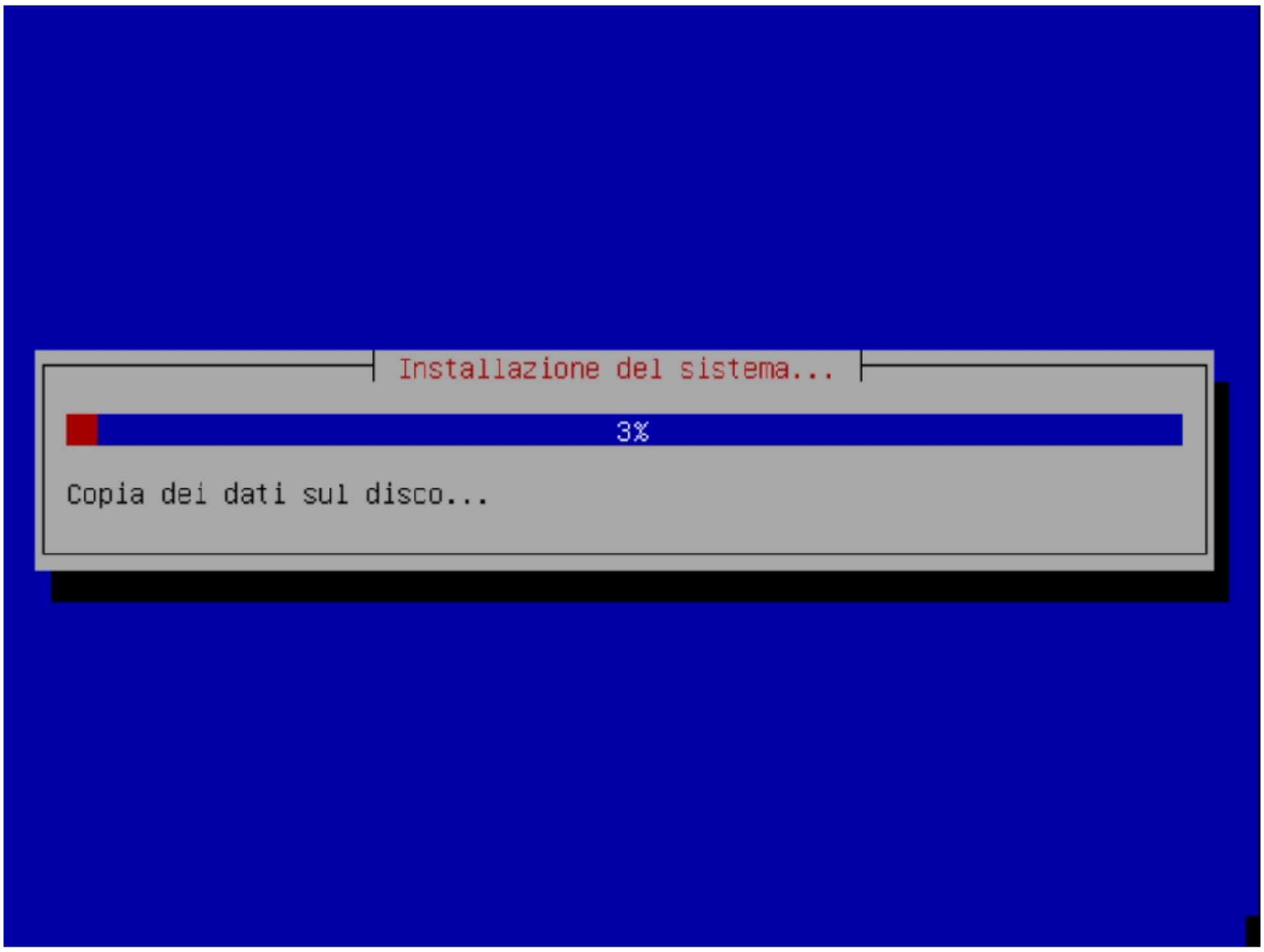

[!!] Partizionamento dei dischi
Modifica della partizione n° 2 di SCSI3 (0,0,0) (sda). Non è stato rilevato alcun file system esistente in questa partizione.
Impostazioni della partizione:
Usare come: File system ext4 con journaling
Punto di mount: /
Opzioni di mount: defaults
Etichetta: nessuna
Blocchi riservati: 5%
Utilizzo tipico: standard
Flag avviabile: attivato
Eliminare la partizione
Impostazione della partizione completata
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti



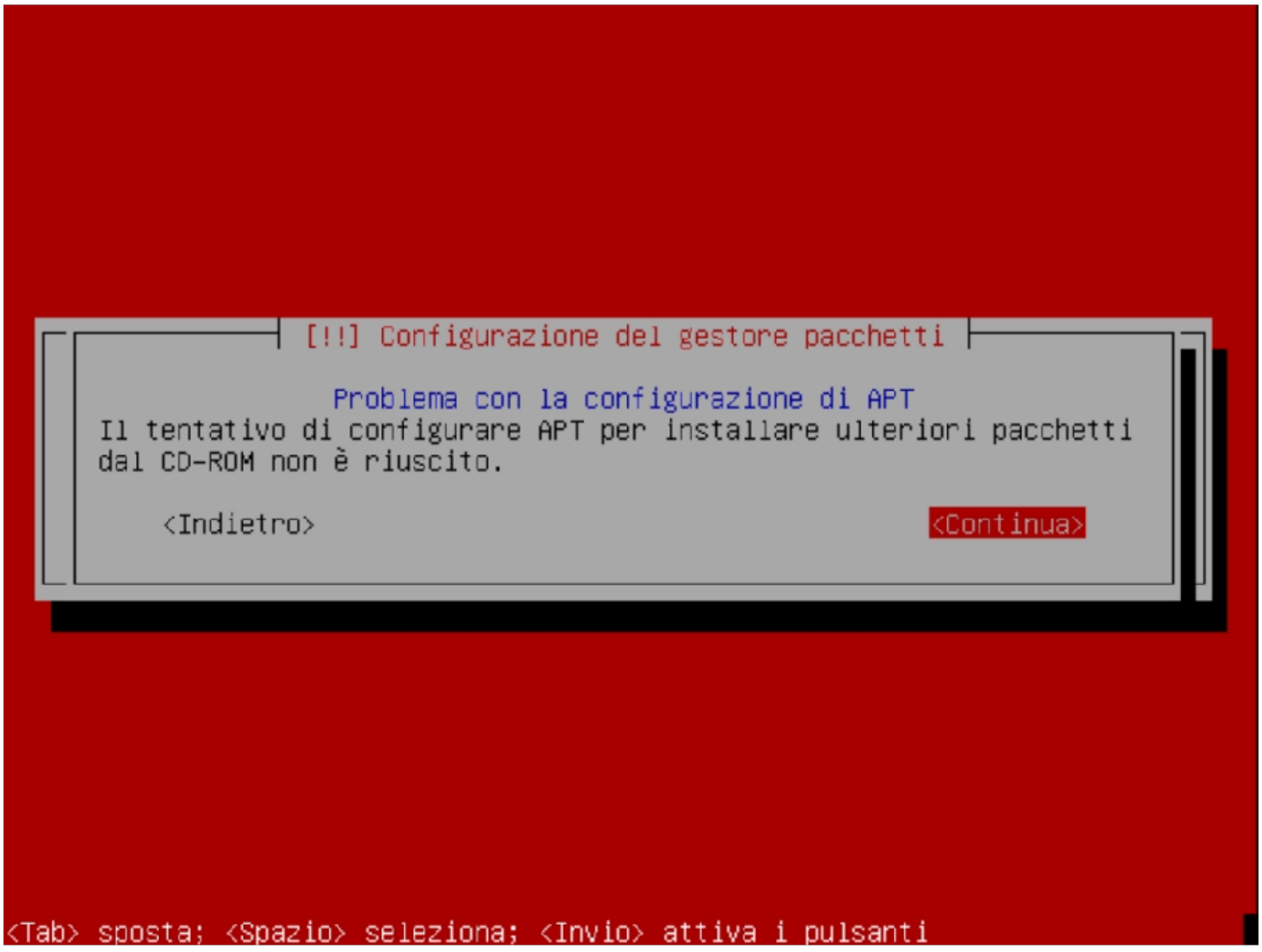
When finished, write the changes to disk.



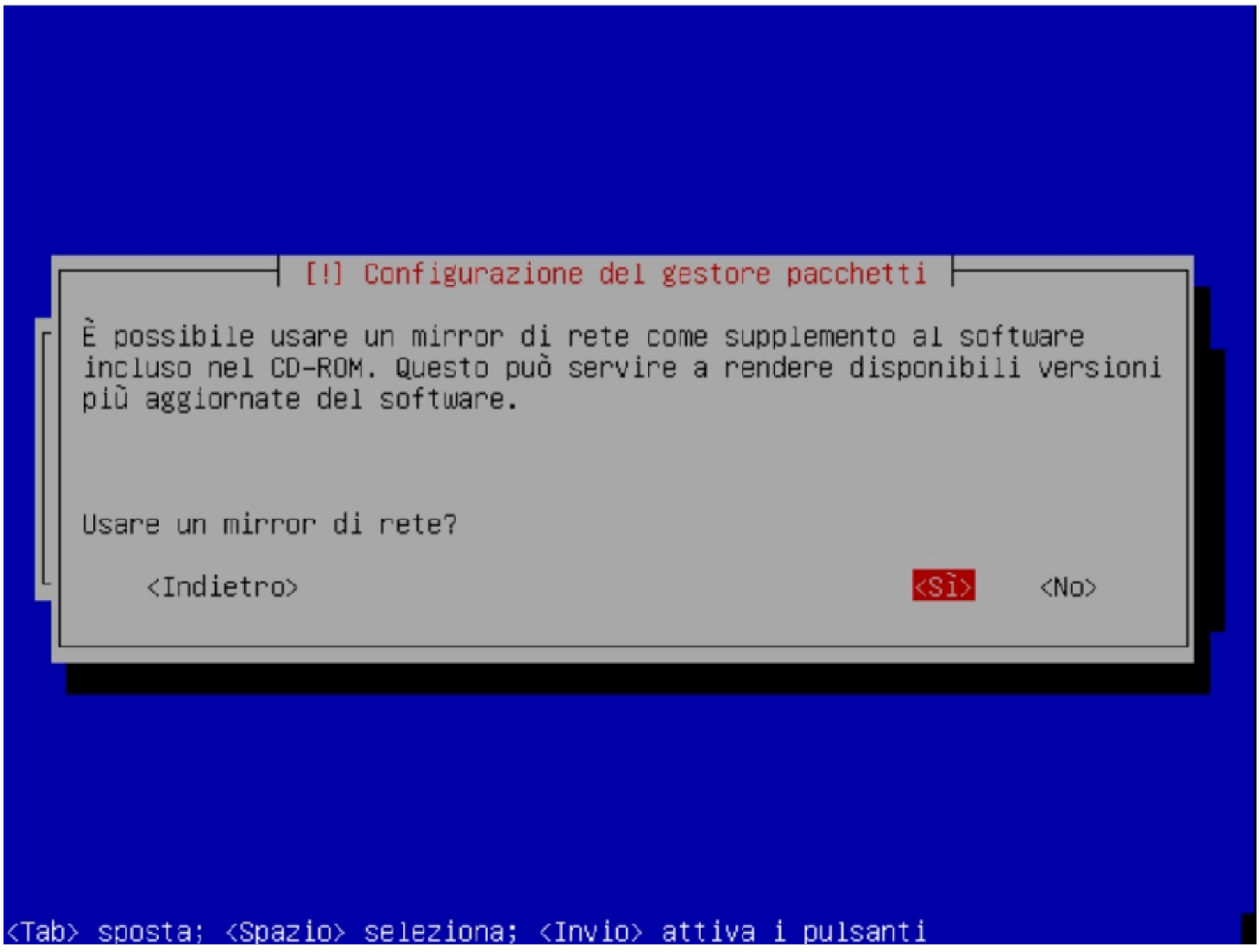
Start the installation of the system.



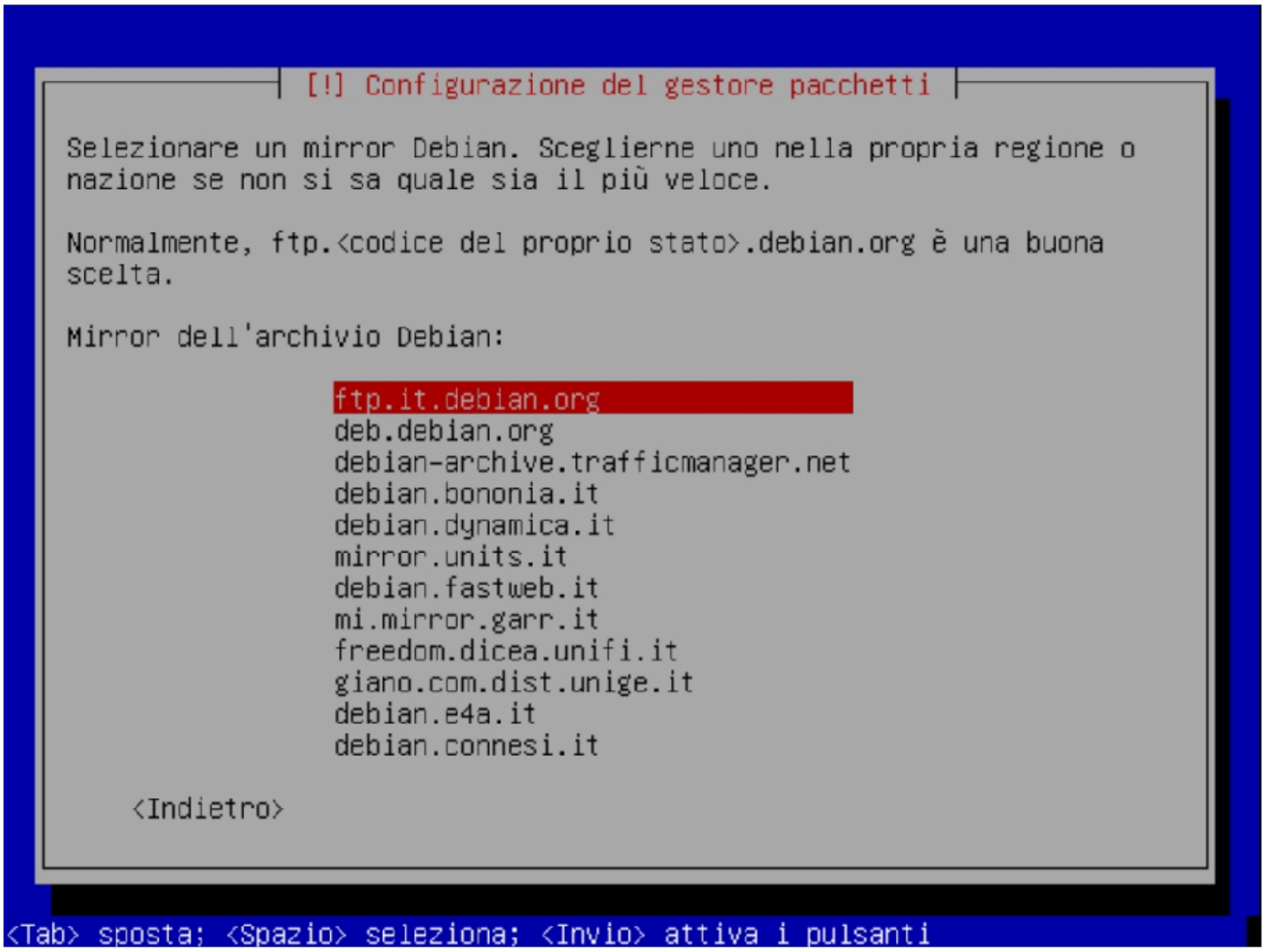
The installer looks for packages in the installation CD-ROM, which does not exist. Simply ignore the error and continue by pressing *Continue*.



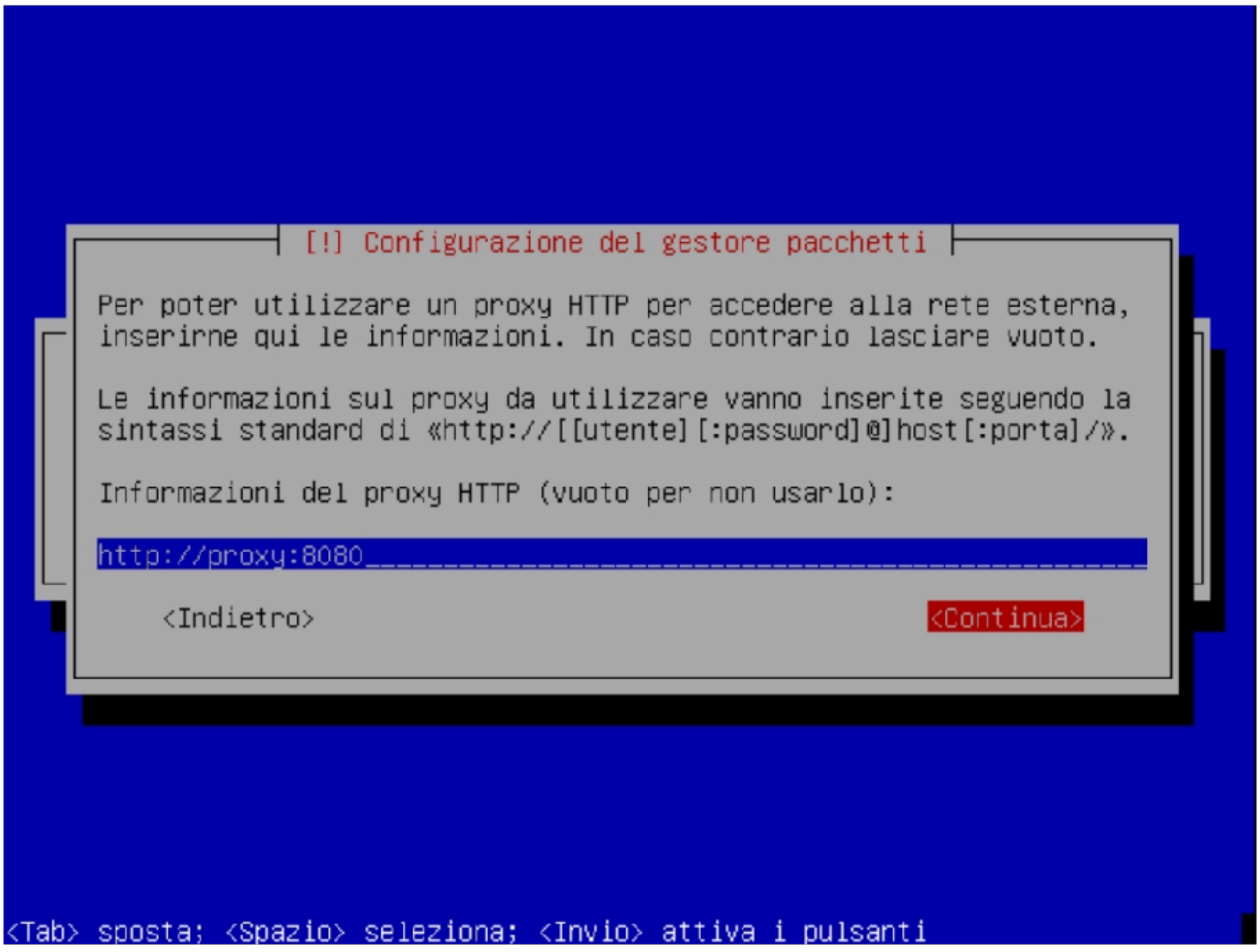
Choose a network mirror.

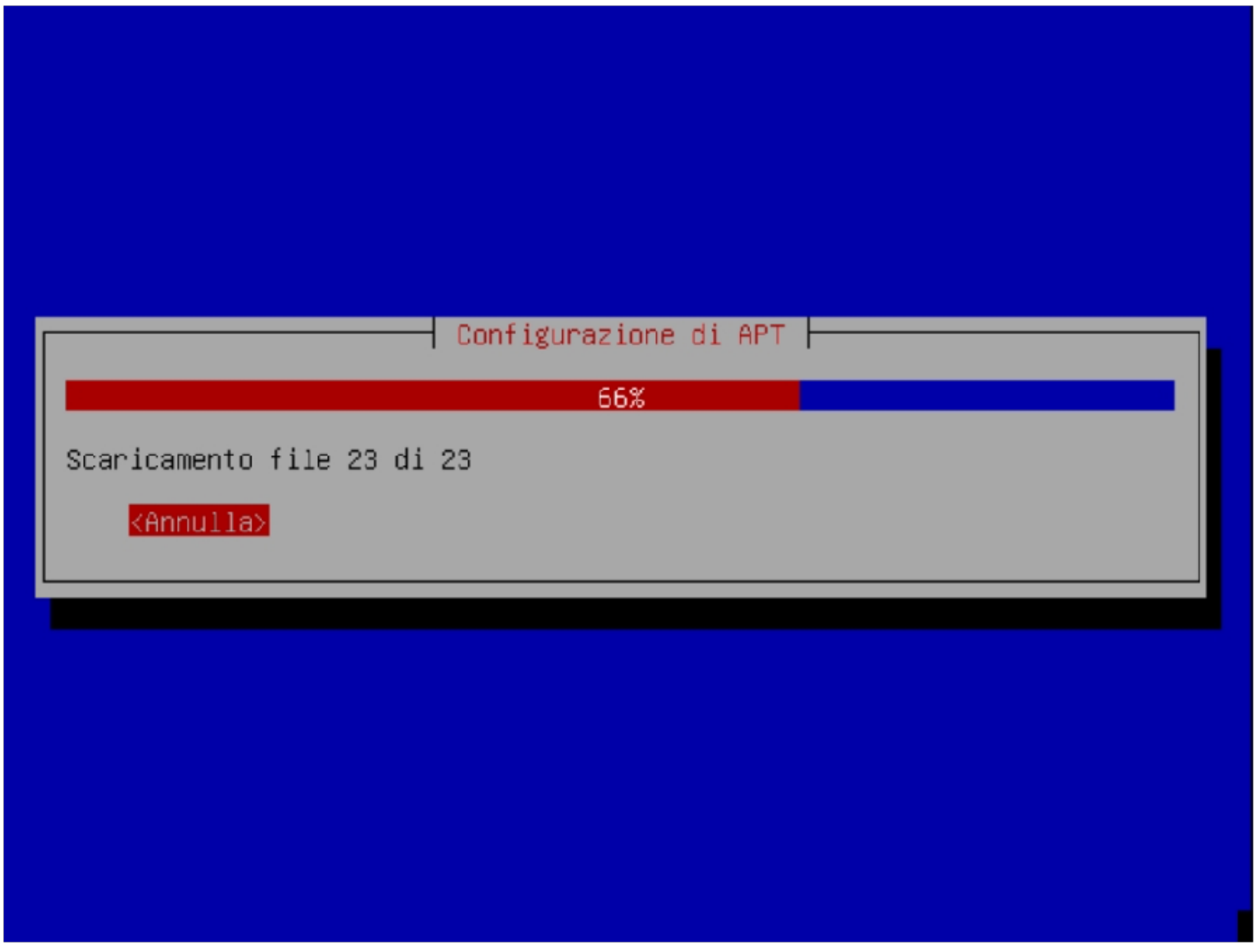

[!] Configurazione del gestore pacchetti
È possibile usare un mirror di rete come supplemento al software incluso nel CD-ROM. Questo può servire a rendere disponibili versioni più aggiornate del software.
Usare un mirror di rete?
<Indietro>
<Sì>
<No>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti


[!] Configurazione del gestore pacchetti
Lo scopo è quello di trovare un mirror dell'archivio Debian che sia vicino alla propria rete. Attenzione perché le nazioni vicine o anche la propria non sono sempre le scelte migliori.
Nazione del mirror dell'archivio Debian:
Estonia
Filippine
Finlandia
Francia
Georgia
Germania
Giappone
Grecia
India
Indonesia
Iran
Irlanda
Islanda
Israele
Italia
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

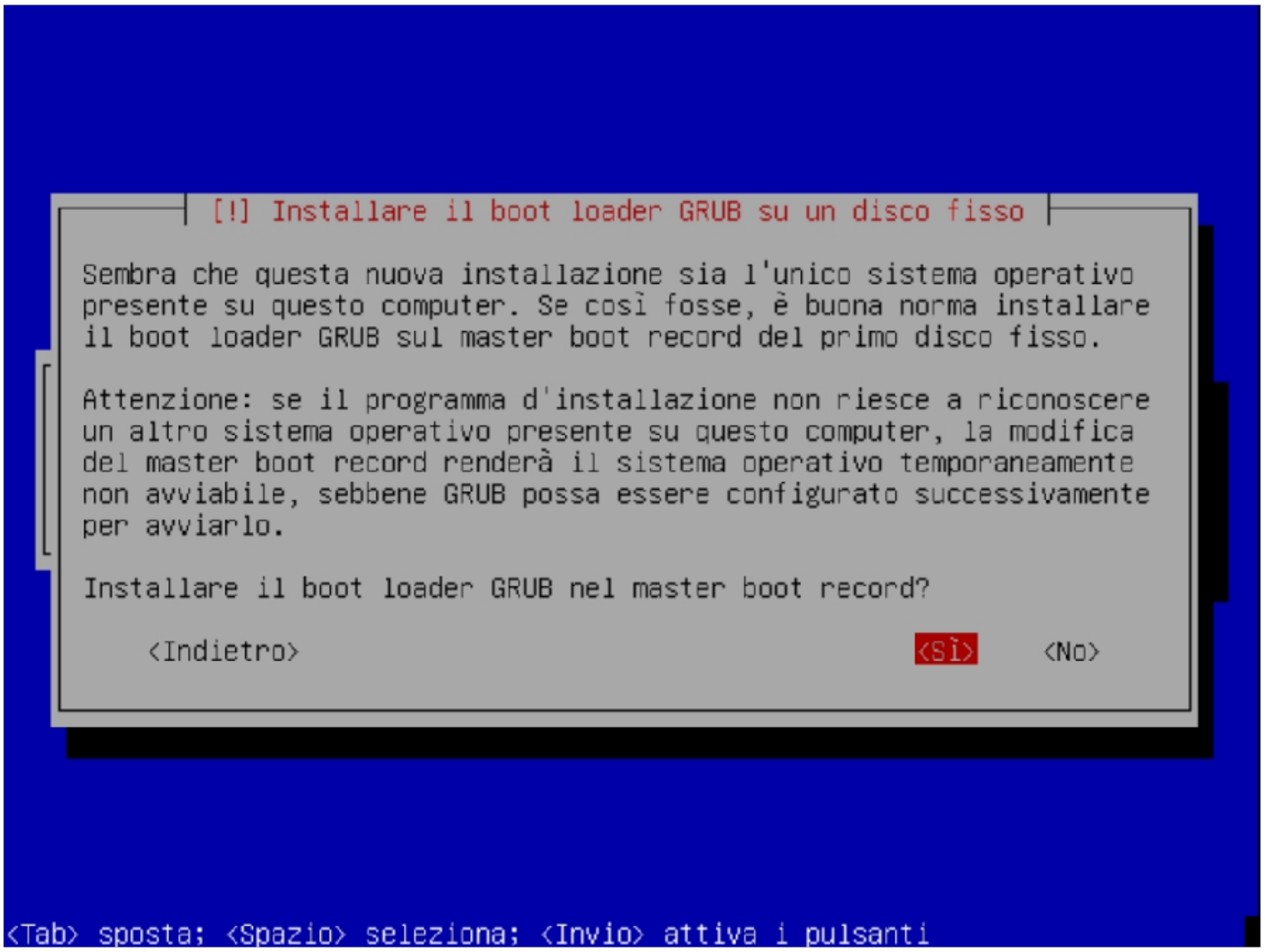


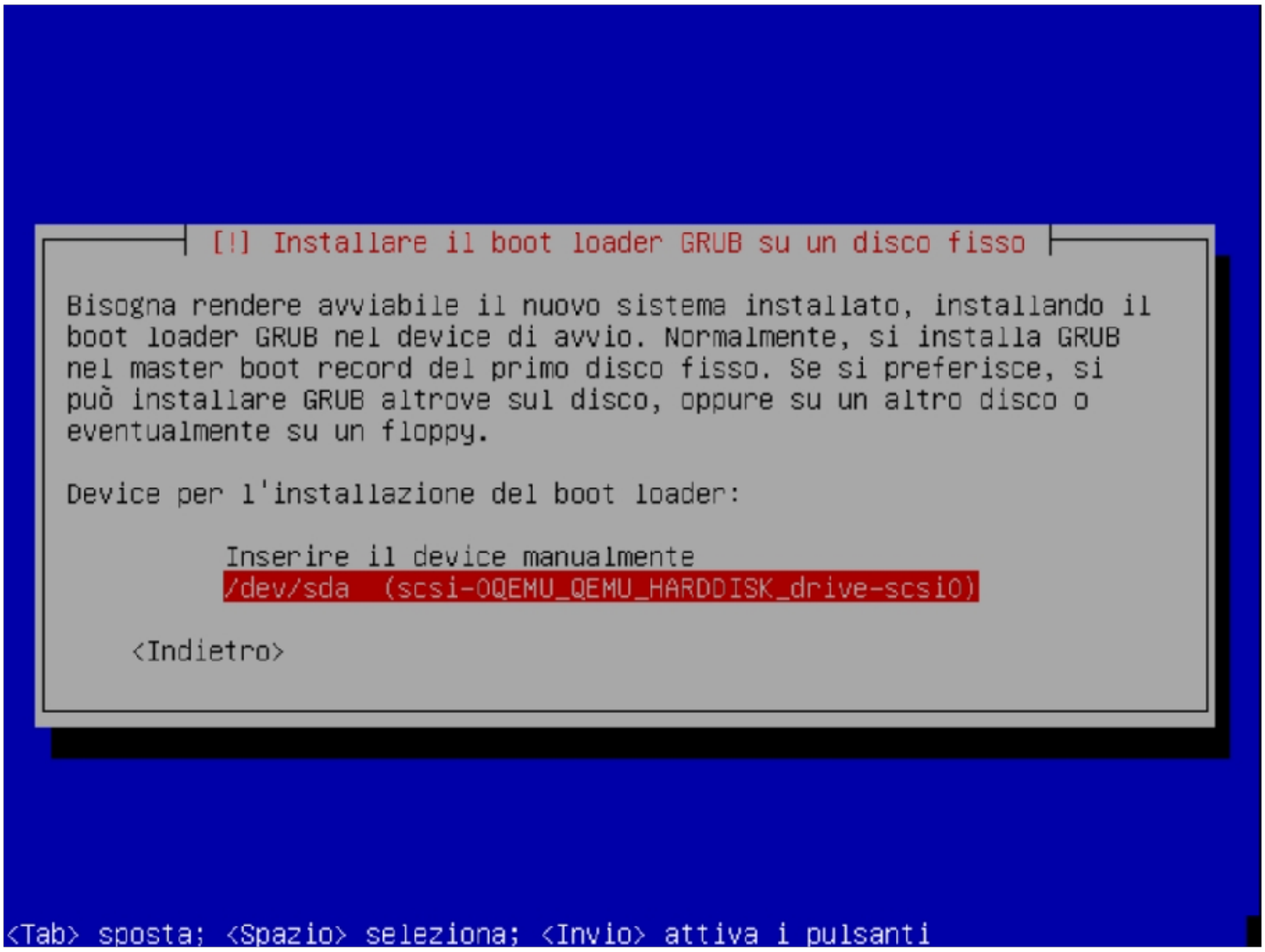
Set the proxy to `http://proxy:8080` where `proxy` responds to FUSS Server.

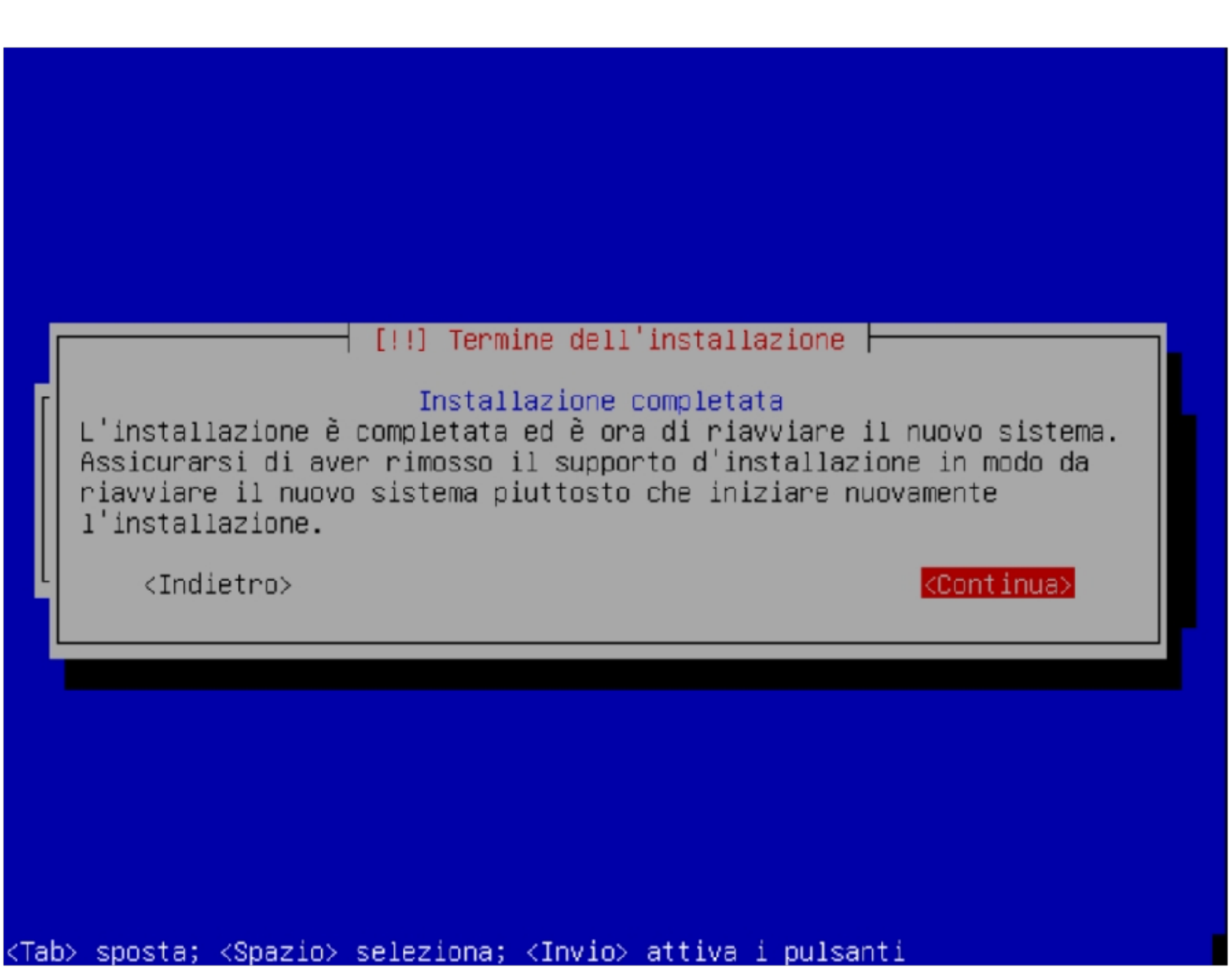

[!] Configurazione del gestore pacchetti
Per poter utilizzare un proxy HTTP per accedere alla rete esterna, inserirne qui le informazioni. In caso contrario lasciare vuoto.
Le informazioni sul proxy da utilizzare vanno inserite seguendo la sintassi standard di «http://[[utente][:password]@]host[:porta]/».
Informazioni del proxy HTTP (vuoto per non usarlo):
http://proxy:8080
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

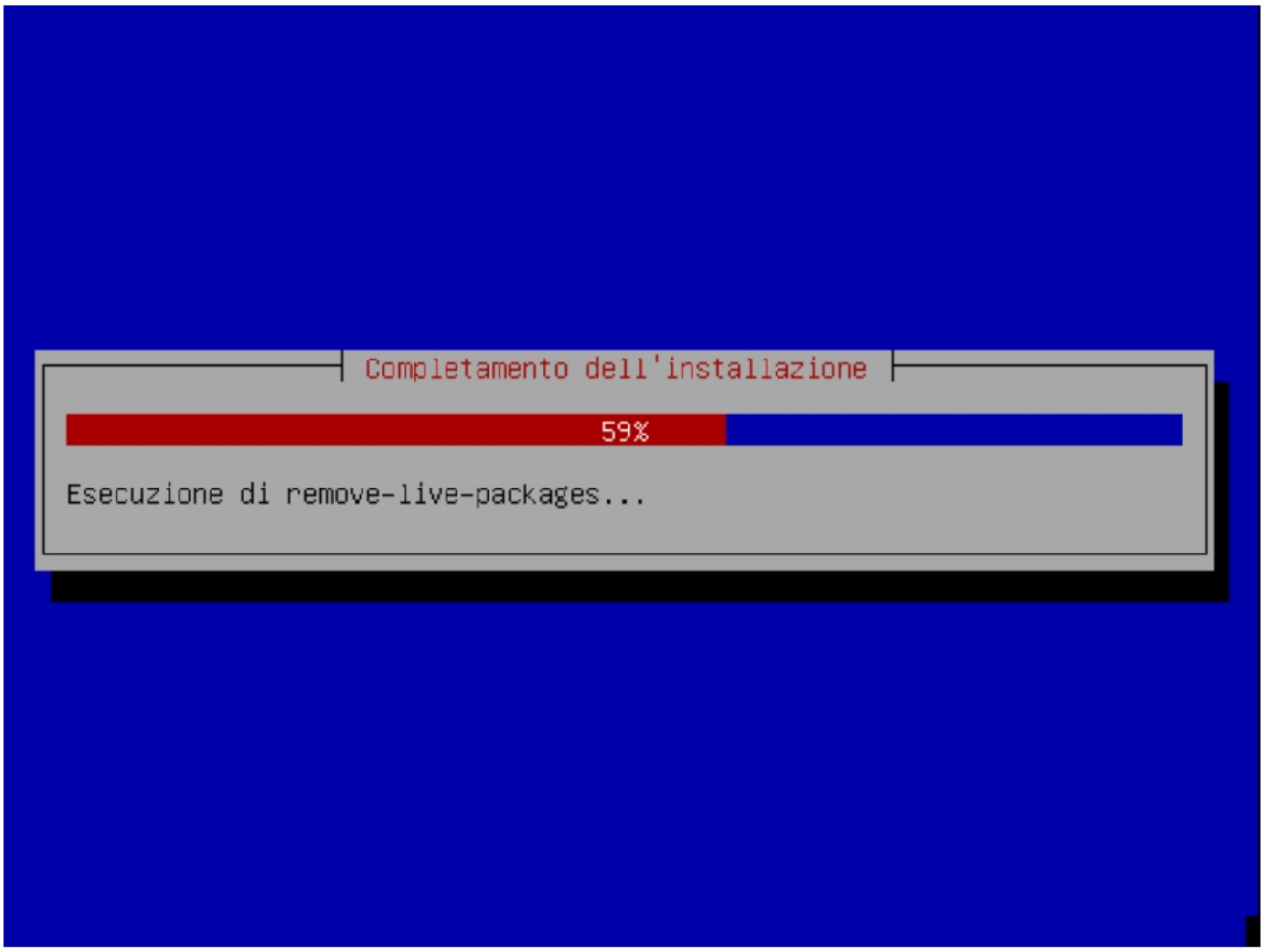

Configurazione di APT
66%
Scaricamento file 23 di 23
<Annulla>

Install the GRUB boot loader in the master boot record of the disk on which you are installing the system.




[!] Installare il boot loader GRUB su un disco fisso
Bisogna rendere avviabile il nuovo sistema installato, installando il boot loader GRUB nel device di avvio. Normalmente, si installa GRUB nel master boot record del primo disco fisso. Se si preferisce, si può installare GRUB altrove sul disco, oppure su un altro disco o eventualmente su un floppy.
Device per l'installazione del boot loader:
Inserire il device manualmente
/dev/sda (scsi-0QEMU_QEMU_HARDDISK_drive-scsi0)
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti


[!!] Termine dell'installazione
Installazione completata
L'installazione è completata ed è ora di riavviare il nuovo sistema. Assicurarsi di aver rimosso il supporto d'installazione in modo da riavviare il nuovo sistema piuttosto che iniziare nuovamente l'installazione.
<Indietro>
<Continua>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti



When finished, the machine should be restarted.

1.4.3 FUSS Client Configuration

After rebooting, log in as root. The default password is `fuss` and you should change it with the command `passwd`.

It is necessary to configure the FUSS repositories. Therefore, enable both FUSS repositories and *bookworm-backports* in `/etc/apt/sources.list`:

```
deb [signed-by=/usr/share/keyrings/fuss-keyring.gpg] http://archive.fuss.bz.it/
↪bookworm main
deb http://httpredir.debian.org/debian bookworm-backports main
```

The sources.list should therefore result in, for example:

```
# See https://wiki.debian.org/SourcesList for more information.
deb http://deb.debian.org/debian bookworm main
deb-src http://deb.debian.org/debian bookworm main

deb http://deb.debian.org/debian bookworm-updates main
deb-src http://deb.debian.org/debian bookworm-updates main

deb http://security.debian.org/debian-security/ bookworm-security main
deb-src http://security.debian.org/debian-security/ bookworm-security main

# bookworm-backports
deb http://httpredir.debian.org/debian bookworm-backports main
```

(continues on next page)

(continued from previous page)

```
deb [signed-by=/usr/share/keyrings/fuss-keyring.gpg] http://archive.fuss.bz.it/
↪bookworm main
```

However, if you need to download non-free packages as well, add "contrib" to " main", "non-free" and "non-free-firmware."

```
# See https://wiki.debian.org/SourcesList for more information.
deb http://deb.debian.org/debian bookworm main contrib non-free-firmware non-
free deb-src http://deb.debian.org/debian bookworm main contrib non-free-
firmware non-
↪free

deb http://deb.debian.org/debian bookworm-updates main contrib non-free-firmware
↪non-free
deb-src http://deb.debian.org/debian bookworm-updates main contrib non-free-.
↪non-free firmware

deb http://security.debian.org/debian-security/ bookworm-security main contrib non-.
↪free-firmware non-free
deb-src http://security.debian.org/debian-security/ bookworm-security main contrib
↪non-free-firmware non-free

# bookworm-backports
deb http://httpredir.debian.org/debian bookworm-backports main contrib non-free-
↪non-free firmware

deb [signed-by=/usr/share/keyrings/fuss-keyring.gpg] http://archive.fuss.bz.it/
↪bookworm main contrib non-free
```

Note: If you are behind a FUSS server, in order for you to download the APT signing key, you must first define- re `export http_proxy=http://proxy:8080` and `export https_proxy=http://proxy:8080`

Install, if not already present, the `wget` package:

```
apt update
apt install wget
```

Add the repository signature key `archive.fuss.bz.it` and update the packages with apt.

```
wget -qO - https://archive.fuss.bz.it/apt.key | gpg --dearmour > /usr/share/
↪keyrings/fuss-keyring.gpg
apt update
apt dist-upgrade
```

If necessary, add the necessary Debian packages depending on the context in which the FUSS Client is installed.

1.4.4 Creating a client image with Clonezilla

In order to speed up the installation of the FUSS Client on the remaining PCs/notebooks, it is recommended to create an image of the first FUSS Client with Clone- zilla. The FUSS Server mounts an instance of Clonezilla, executable from any machine on the LAN via PXE Boot (network boot). Therefore, restarting the newly created FUSS CLient and choosing the "PXE Boot" boot option will load Clonezilla from the server and allow you to create a first client image that will be saved in the `/var/clonezilla` folder on the server. Clonezilla will ask for the clonezilla user password, which is stored on the server in the `/root/clonezilla_cred.txt` file.

After the process of saving the clone to the server is complete, you can easily install new clients by similarly

launching Clonezilla via network boot and choosing to restore an image.

Each client must be given a different hostname. Therefore, it is necessary to take action on the files `/etc/hostname` and `/etc/host` by restarting the client when finished.

1.4.5 Join the client to the server

Finally, a join of the client to the server must be made by running the `fuss-client` command from the terminal as follows:

```
fuss-client -a
```

As the only interaction it is asked, if configured, which cluster to associate the host with (e.g., *classroom-01*, *classroom-teachers,* etc.). In addition, the server root password must be entered three times.

1.5 Installation with FUSS- FUCC

FUCC stands for Fully Unattended Clonezilla Cloning.

1.5.1 Compilation of the computer list

In the `/srv/clonezilla` folder (normally the standard clonezilla folder) or on other folder on the FUSS server that contains the images to be cloned, you will find the file `computerList.txt` in which you have to list the **no- mi you** want to assign to the computers by specifying the **mac-address** and **the clonezilla image** you want to install on the computer. If you want to hook the computer to the domain you have to add the word **join** and, as the last parameter, the **cluster** name. The file included in the package contains a small commented example, which we give below:

```
info-pc01 08:00:27:ab:5a:a2 cloneImage-img join clustername
```

The creation of the `/srv/clonezilla/computerList.txt` file can also be done automatically by running the script:

```
fuss-fucc octolist NAME-IMMAGE-CLONEZILLA.
```

The file **computerList.txt.octo-new** is created and can be copied instead of `/srv/clonezilla/computerList.txt`. Verify that the list contains all the pc's you intend to update.

This way, if you reinstall in automatic mode, clients are assigned the same hostnames and clusters as before.

1.5.2 Client installation

Once you have done the above, start in `network boot(PXE)` the PCs to be installed (usually you press the `F12` key but it may vary depending on the computer).

The menu presents two possible choices, **automatic** or **manual** , as shown in the screenshot below. **Automatic mode is the default** but obviously requires that the `computerList.txt` file be filled in correctly.

In automatic mode you need to do virtually nothing, the image is copied, the client is renamed and joins the network as indicated in computerList.txt.

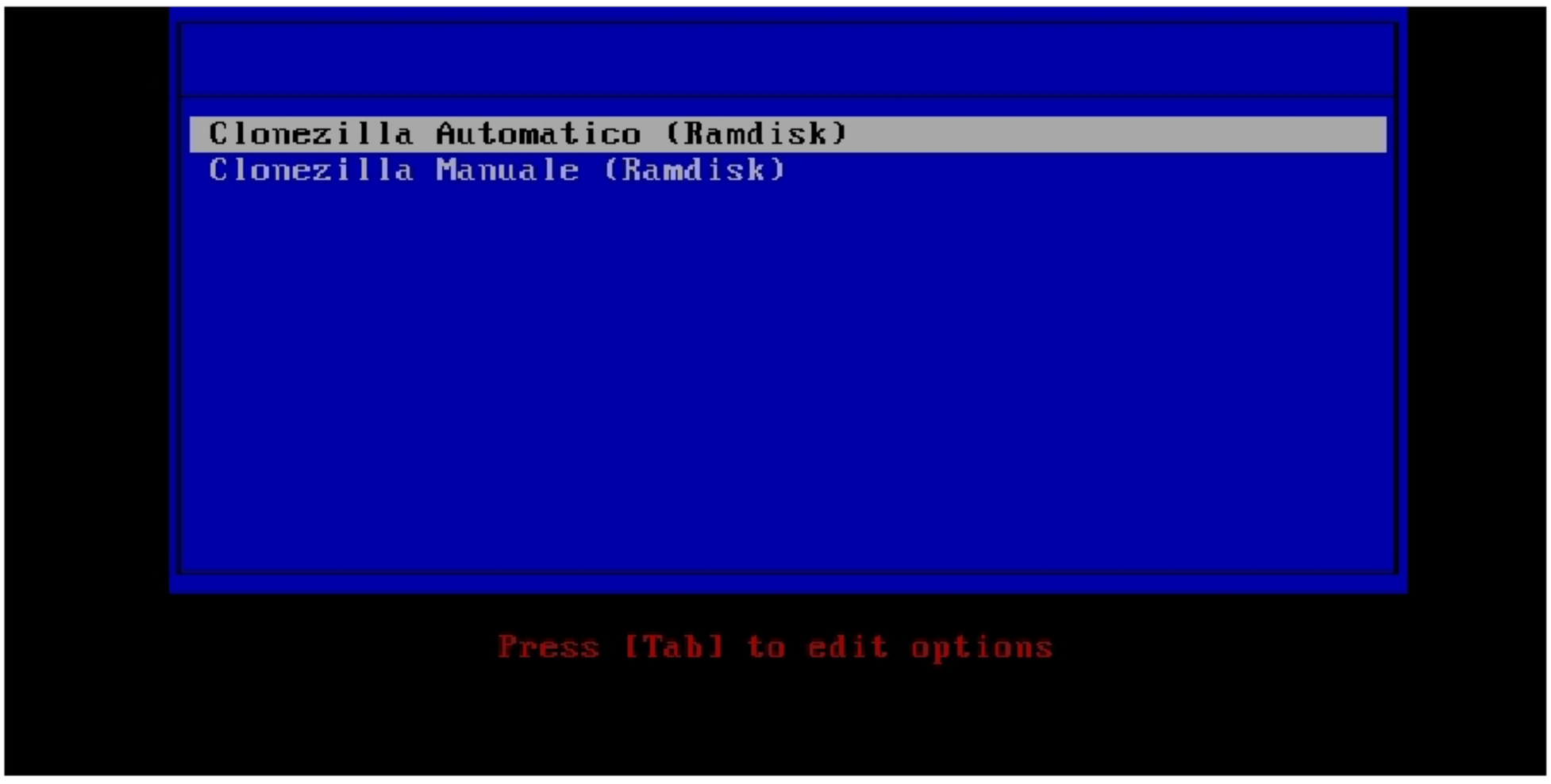


Fig. 2: clonezilla boot

Otherwise, or if something goes wrong, you can opt for manual installation. In that case the client loads clonezilla, but otherwise you install the client almost as if you were using a thumb drive, the partition containing the images is mounted upon password authentication (you choose `skip` when choosing the source).

Cloned image will need to be launched:

```
fuss-client -H <hostname>
```

To rename the client and hook it up to the server.

1.5.3 Configuring automatic root password change

FUCC can automatically change the root password of cloned clients to an encrypted one that is passed to it. To **configure** the `password change` run the script on the server:

```
fuss-fucc rootpw
```

and enter twice the root password to be given to the clients. Normally this **script** must obviously be run **Before** starting to clone the machines.

1.5.4 Access to the OctoNet administration interface

By opening the browser from any PC/notebook on the LAN at http://proxy:13402, the OctoNet educational network configuration interface can be accessed, and from this, among other functions, educational network users can be created. The administrator is the *root* user and the password is the Master Password set while running fuss-server.

This mode, however, results in all traffic going unencrypted, so it is strongly discouraged; use an SSH tunnel as explained in the section on using OctoNet, which does not expose you to the risk of intercepting login credentials.

1.6 Captive Portal/Network Management WiFi

Installation of the captive portal should be done once you have properly installed the *Fuss Server* (according to the instructions in *Installing Traditional FUSS Server*). In particular, it is assumed that the network interfaces for the internal network (the one facing the classroom machines) and external network (the one from which the Internet is accessed) are already correctly configured.

In order to use the *Captive Portal, it* is necessary to have a third network interface that can be left **unconfigured**. This interface will be the one that must be physically attached to the network section (which must be physically separated from the server's internal network) that will be managed by the *Captive Portal* (for example, an access point can be attached to it without authentication). In the following examples we will assume `ens20`.

Keep in mind that the configuration of the physical interface handled directly by `fuss-server`, so take care to verify that network manager has not been activated on *Fuss Server* when installing the graphical interface (the default in any case does not). The program performs the configuration in the file `/etc/network/interfaces.d/90-wifi-fuss` so that it is compatible with any confi- guration created by `cloud-init`. If other manual configurations are present (as previously stated in `/etc/network/interfaces`) these should be removed.

To install the necessary to manage the Wi-Fi network with the new infrastructure, the command must be executed:

```
fuss-server cp
```

which will request, if not already defined, the data needed for configuration. As with the others these are maintained in the file `/etc/fuss-server/fuss-server.yaml` In particular they will be required:

- Network interface on which to attest the *Captive Portal* network (e.g. `eth2`)
- *Captive Portal* network address (e.g. `10.1.0.0/24`) An example

of an installation session is as follows:

```
root@fuss-server-iso:~# fuss-server cp
################################################################################
Please insert Hot Spot Interface

The Hotspot interface of the server, ex. 'eth3'
Your choice? ens20
################################################################################
Please insert Hot Spot Network (CIDR)

The Hotspot network of the server, ex. '10.1.0.0/24'
Your choice? 10.1.0.0/24
...
```

Note: Keep in mind that in the installation DHCP leaves the first and last twenty addresses of the indicated network free, which can be used to assign static addresses to any devices (such as access points).

The new management system provides access to the Internet only through the web proxy, which is configured automatically with user authentication on LDAP (so you need to have a user defined to try it), and allows only authenticated users to log out, passing through the proxy for web traffic.

For *Captive Portal* operation, the `fuss-captive-portal.conf` file is also created by the installation command, which contains the variables needed by the firewall script to manage *Captive Portal-related* accesses; this file must not be modified or deleted, otherwise restarting the firewall will not open the accesses needed for *Captive Portal* operation.

Note: Installing the captive portal adds the `wifi` group (see the two files `/etc/ group` and `/etc/octofuss/octofuss.conf in this regard`). By default, users in a school network do not belong to

---

to the `wifi` group and therefore do not have permission to access the captive portal; they must be explicitly authorized in OctoNet.

CHAPTER 2

Architecture

2.1 Services present on Fuss Server

Table 1: Services

Service	Description
apache	Web server
bind	Local DNS
e2guardian	Internet content filter (if not disabled)
isc-dhcp-server	DHCP for local area network
iptables	Firewall
fuss-fucc	Management of automated client installation
fuss-manager	Machine manager on local area networks (new experimental version)
kerberos	Authentication and authorization
ldap	Authentication
nfs-kernel-server	Shared Home
Octonet	Management of machines and users (legacy)
Samba	File Sharing
squid	Web proxy

CHAPTER 3

3.1 Configuration of server

Once the basic installation of the machine is complete, care must be taken to properly configure the network, identifying the internal (the one facing the classroom machines) and external (the one from which the Internet is accessed) network interfaces. You must also set up the hostname and the name and domain of the machine you are working on.

Warning: Setting the machine hostname to its final value before running configuration procedure is important; changing the setting later is problematic. This is usually done when installing the operating system, but if this is not what is desired the correction must be applied **before** running the `fuss-server` command. The hostname of the machine in fact is used in the configuration playbook for the creation of various files that are then referenced, changing it later may not have an immediate impact in the operation of the server, but it may in the next run (e.g., for updating) of `fuss-server`.

To perform configuration creation, it is necessary to execute the command:

```
# fuss-server create
```

this, if a configuration has not been done before, will ask for a set of data. In particular, the following will be requested:

- The local network that will be used (e.g. 192.168.1.0/24);
- The domain name of the network (e.g., school.bzn);
- the workgroup for the windows domain (e.g., SCHOOL);
- an address range for DHCP (e.g. 192.168.1.10 192.168.1.100);
- the server's master password (use a long and complicated one!);
- the location (e.g., Bolzano);
- The interface of the external network (e.g. ens18);
- The internal network interface (e.g. ens19);

The data request program will use the text interface in the terminal.

At the end of the entry, a check for correctness of the entered data will be performed; if there are any problems, a new entry window will be re-entered with only the problematic data, until a completely valid configuration is obtained.

Finally, the program will automatically proceed to configure everything necessary, including any installation of dependencies.

If you don't want this to happen, for example because you want to change right away the default parameters with which the installation takes place, you can run instead of `fuss-server create` the `fuss-server configure` command, which only performs the request for the previous information and generates the corresponding configuration file `/etc/fuss-server/fuss-server.yaml`; it is in this file that you will then have to redefine (with respect to the values contained in `/etc/fuss-server/fuss-server-default.yaml`) the control variables that you want to change. Once the changes have been made you can move on to configuration by launching then `fuss-server create`.

In case the program stops due to temporary problems (e.g., a drop in the Internet connection), it is possible to relaunch it with: `fuss-server create`; of course, you will not be asked to configure it, but the program will proceed with its automatic step.

3.2 Access to server

Access to the server is allowed not only from the console, but also via SSH, for the root user, with key authentication. The keys must be installed in the file `/root/.ssh/authorized_keys`.

Normal users can access the server in SSH with their own username and password only if they are part of the `sshaccess` group. The group is created as a local group on the server when running `fuss-server` and SSH is configured for access in `/etc/ssh/sshd_config` with the line:

```
AllowGroups root sshaccess
```

which provides access to root and group members.

This setting is done by the `fuss-server` command with using an ansible `blockinfile` directive, any changes made within the block will be overwritten on a subsequent invocation of the command. The use of the `AllowGroups` directive is incompatible with the use of `AllowUsers`, which therefore should not be used.

To provide SSH access to users, it will be sufficient to add them to the local `sshaccess` group with the command: `adduser user sshaccess`.

Note: if the localadmin user can't get into SSH on the server check that they belong to the group `sshaccess`

3.3 The main files of configuration

Under `/etc/fuss-server` are installed a number of files that maintain configuration data used by the server services, detailed in the following paragraphs, managed through `octofuss`. Obviously they must not be deleted, or the services they refer to will fail.

3.3.1 Fuss Server Configuration Files

In the file `/etc/fuss-server/fuss-server.yaml` is the general configuration of the Fuss Server. The format is an ansible variable file i.e., a simple key-value dictionary in yaml, for example:

```
key: value other_key: new
value
```

It must contain the default values described in *Server Configuration*; unlike the other files it can be deleted, in which case it is recreated from an empty example.

To change the settings in that file, you can also launch:

```
# fuss-server configure -r
```

(the `-r` option is necessary, because if the settings are present the program does not require them).

To apply the changes launch:

```
# fuss-server upgrade
```

which will do the consistency check of the values in the file and apply them to the system.

Since the file can be rewritten by the fuss-server command, it should not be used for additional configurations, for which there is instead the file described in the next section.

3.3.2 Fuss Server defaults file

Under `/etc/fuss-server/` is also installed second file, `fuss-server-defaults.yaml`, also in yaml format, in which other variables can be set to customize the installation.

This file can be empty (the default version installed by the package contains only comments), but it must not be deleted, otherwise `fuss-server` will give error by not finding it.

The following table describes the variables that can be defined in this file to control certain characteristics assumed by the installation.

Variable	Meaning	Contenu-to	De-fault
`dans_maxchild`	Maximum number of e2guardian child processes.	Whole	600
`proxy_win_exclude`	Configure Squid to exclude Windows clients.	String	yes
`dans_exclude_localnet`	Excludes the local network from the filtering of e2guardian.	String	yes
`dhcp_default_lease_time`	Default duration of a dhcp lease.	Whole	86400
`dhcp_max_lease_time`	Maximum duration of a dhcp lease.	Whole	172800
`squid_filedescriptors`	Maximum number of filedescriptors per squid	Whole	10240
`e2guardian_install`	Whether or not to install e2guardian	Boolean	yes
`e2_nofile`	Open file limit for e2guardian	Whole	8192
`e2_workers`	Limit of httpworker for e2guardian	Whole	1024

It is possible to change these default values so that the relevant configuration will not be changed if the fuss-server is upgraded, e.g. if you want to rehabilitate Internet access by Windows machines you can change the value of `proxy_win_exclude` from `yes` to `no`, or if you want to rehabilitate content filtering on the local network (not necessary in the project schools due to the presence of upstream filtering) you can change `dans_exclude_localnet` from `yes` to `no`.

Every time a change is made to one of these variables, for the relevant configuration to be appli- cated, it will be necessary to run `fuss-server upgrade`. Since `fuss-server-defaults.yaml` is marked as a configuration file, it will not be overwritten if the package is upgraded and the changes made will be retained.

3.3.3 DHCP Server

The file `/etc/dhcp/dhcp-reservations` contains the static address assignments for the client , which is included in the configuration and installed empty when creating the fuss-server. The contents of this file are managed through octofuss and use the format provided by `dhcp.conf` for "_reservations_", i.e., a series of entries in the form:

```
host nomeclient {
        hardware ethernet 00:XX:XX:XX:XX;
        fixed-address
        nomeclient.domain.co.uk;
}
```

Whether nomeclient.domain.co.uk is defined in the DNS, or:

```
host nomeclient {
        hardware ethernet 00:XX:XX:XX:XX;
        fixed-address IP.AD.DR.ES;
}
```

using an IP outside the range of DHCP (which by default takes addresses between 1/4 and 3/4 of the network used for the LAN). If the `/etc/dhcp/dhcp-reservations` file isdeleted, the service is not started.

3.3.4 Firewall

The configuration files for the firewall are all in the format:

```
value:description
```

with the exception of the one describing allowable internal machines and reachable external services, which is in the form:

```
host:service:description
```

Lines beginning with a # are considered comments and are ignored, and also whatever does not appear within the block marked `ANSIBLE MANAGED BLOCK` is not overwritten by the re-execution of the fuss-server installation command.

If you specify a host this must be either a domain name or an IP address, however, keep in mind that the firewall performs IP address resolution at startup, so using a domain name is risky, especially when several addresses may correspond to it (e.g. www.google.com) because the firewall will only refer to the one resolved at startup.

When specifying a service instead this must be in the port/protocol form (e.g., 123/udp or 2628/tcp). Lower case and numeric values are recommended.

The description can be omitted, a standard description will still be inserted.

The files used are as follows; they are enabled on firewalls in the sequence in which they are shown in the table (this means that a host in the first file will still not be able to reach any external services, even those made accessible with the other files):

File	Content	Format
`/etc/fuss-server/firewall-denied-lan-hos`	Hosts that cannot reach any services on the network tinsternet	IP-address
`/etc/fuss-server/firewall-allowed-lan-ho`	List of hosts that can access network services `sinttsernet` without any filter and/or limitation	IP-address
`/etc/fuss-server/firewall-allowed-wan-ho`	List of hosts on the Internet network that can be accessed without any filter and/or limitation	IP-address
`/etc/fuss-server/firewall-allowed-wan-se`	Services on the Internet network that can be accessed without rlivmiitcaezisoni and/or control. The ports to be used for service must be indicated.	por-ta/protocol
`/etc/fuss-server/firewall-external-services`	Services offered by the server on the external network `ces`	por-ta/protocol
`/etc/fuss-server/firewall-allowed-wan-ho`	Services on the Internet network reachable from specific hosts of the sctesinetrervniacseensza mlimt	IP-address:port/protocol

Remember that after making manual changes to the above files you must relaunch the firewall for them t o take effect, with:

```
/etc/init.d/firewall restart
```

In case you have also installed the Captive Portal, the firewall uses the additional file `/etc/fuss-server/fuss-captive-portal.conf`, to obtain the network used by it and enable the necessary accesses. Said file must not be deleted, otherwise the aforementioned accesses will be missing and the Captive Portal will not work if the firewall is restarted.

3.3.5 squid (web proxy)

The file `/etc/squid3/squid-added-repo.conf` allows you to add websites to the acl `repositories` To which access is always allowed without authentication.

Content must be of the form:

```
acl repositories url_regex XXX
```

where `XXX` is the regular expression representing the site we want to enable; examples of the syntax can be found in `squid.conf`, such as:

```
acl repositories url_regex ^http://.*.debian.org/.
```

3.3.6 e2guardian (content filter)

A list of sites that are nevertheless granted access by e2guardian (successor to Dansguardian) is maintained in the file `/etc/fuss-server/content-filter-allowed-sites`. This list can also be managed from the *OctoNet* web interface from the *Web Filter* menu, which also allows other configuration files to be configured under `/etc/e2guardian/lists/`.

Caution: content filtering requires significant resources on the server; in schools where upstream protection is already in place, it may be convenient to exclude local network IPs from filtering by adding to those files the ranges of PCs to be excluded or individual IPs if those PCs have static IPs.

3.3.7 dhcpd

The `/etc/dhcp/dhcpd-added.conf` file allows you to add dhcp daemon configuration parameters beyond what is handled by the fuss-server.

That file is loaded at the end of `/etc/dhcp/dhcpd.conf`, and shares its syntax.

3.3.8 bind (DNS)

The file `/etc/bind/named.added.conf.local` allows you to add bind configuration parameters beyond what is handled by the fuss-server.

That file is loaded at the end of `/etc/bind/named.conf.local`, and shares its syntax.

3.4 Updates

Since version 8.0, the operation of fuss-server create has been changed and it is now possible to launch fuss-server create multiple times: the changes already applied remain constant.

3.4.1 System Updates

System updates can be performed manually using Debian's ordinary mode, that is, by connecting to the server as root and executing the commands:

```
# apt update
# apt
upgrade
```

responding positively to the request to install the updated packages.

3.4.2 Minor updates to fuss-server

In case there are minor version updates (10.0.x → 10.0.(x+1)) of fuss-server to apply it is enough, from root:

- Download and install the updated package:

```
# apt update
# apt install fuss-server
```

- Reapply the new configurations:

```
# fuss-server upgrade
```

3.4.3 Updates to configuration files

`fuss-server upgrade` restores the contents of many configuration files to the desired values for the fuss-server.

For some services for which it is more common to have to maintain local changes there are files on purpose, included by the general file and untouched by `fuss-server`, but this is not true in every case.

However, when a configuration file is modified, a backup copy is saved in the form- to `<filename>.<a number>.YYYY-MM-DD@HH:MM:SS~`; any customizations to be restored can be retrieved from this file.

To find the modified files immediately after launching fuss-server you can use the command:

```
# find /etc -mmin -10
```

which finds all files modified in the last 10 minutes.

To find all the backup files generated by `fuss-server update` in 2020 you can use instead:

```
# find /etc/ -name "*.*.2020-*@*~"
```

or, to be more precise and find the June 2020 changes, for example:

```
# find /etc/ -name "*.*.2020-06*@*~"
```

Warning: Simply copying the old configuration file to the new one is a discouraged practice: generally updates introduce changes to such files in order to improve fuss-server operation or fix bugs, and undoing such changes negates that benefit.

Rather you should check the changes between the two versions of the file, for example, with:

```
# diff <file name> <backup file name>
```

and reapply only what is actually needed for local installation.

3.5 Backup with fuss- backup

The `fuss-backup` package installs a new borg-based backup program that at the same time also provides dump functionality for databases (LDAP, any MySQL and Postgres) installed on the server. For these ul- tives, a dump is created under `/var/backups` (in the subdirectories `slapd`, `mysql`, `pgsql`, respectively) in which the last seven text dumps are maintained for immediate access. The `/var/backups` directory is included by default in the backup to external disk or NAS.

3.5.1 Backup scheduling

For backup scheduling, the CRON file `/etc/cron.d/fuss-backup is` installed from the package in which the backup script is scheduled to run every Monday at 1:15 pm. The backup can be run manually (by invoking the `fuss-backup` command) at any time.

The external device is mounted before the backup is performed and dismounted upon its completion. This allows, in the case of external disks, a removal and eventual rotation.

3.5.2 Configuration

For the backup to work, a valid configuration is required in `/etc/fuss-backup/ fuss-backup.conf`. In particular, the variable `START=yes` must be set and indicated in the variable `DISK` the device on which the backup is run (more details later).

> **Warning:** installing the package installs a configuration file that blocks the backup from running (`START=no` and `DISK` empty), so you need to do the configuration manually since the name of the external device to which you make backups is not known a priori.

Configuration variables

The following table shows the variables in the configuration file and their meanings. They have been commented in the file with further details.

Variabi- the	Meaning	Default
START	if different from `yes` the backup is not run	no
DISK	the device on which the backup	blank
PATHS	the directories being backed up (space-separated string)	`/etc /home /var/backups /var/lib /. var/log /var/mail /var/local`
MAIL- TO	addresses to email the results to	root
RETEN- TION	Minimum number of backups (1 per day) from keep on file (internal use)	7
BASIC- DIR	directory where to mount the storage	`/mnt/backup`
BAC- KUP_DIR	sub-directory of the previous one where to create the archive	`borgdata`
RECO- VER- DIR	directory where to mount backups for the recovery	`/mnt/recover`

Example of configuration

Therefore, the following steps are essential to configure and activate backup by editing `/etc/fuss-backup/fuss-backup.conf`:

- define `START=yes`
- define an appropriate value for DISK, for example, if you have an external disk you will have to indicate its device name, e.g.:

```
DISK=/dev/sdc1
```

  if you have a NAS you will need to indicate the IP address to which it is reachable and the directory that it exports to NFS with the syntax `IP.DEL.NAS.LOCAL:/directory/exported/dalnas`, e.g. in the case of the NAS-QNAPTVS653 used for testing you will have:

```
DISK="192.168.10.5:/share/CACHEDEV1_DATA/Public"
```

To find the directory exported to the NAS-QNAPTVS653 one can connect to it with SSH and examine the contents of the `/etc/exports` file, the contents of which reflect the directories defined in the "Shared folders" section of the WEB-accessible control panel (in the case illustrated the one available was Public).

The format of the `/etc/exports` file provides for one exported directory per line (one must be chosen if there are several), with fields separated by spaces; the first field is the directory to be used in the `DISK` variable (in the case in example precisely `/share/CACHEDEV1_DATA/Public`).

As an additional configuration, the directories of the server whose backup is desired can be listed by modifying the `PATHS` variable, to be specified in the form of a space-separated list, for example:

```
PATHS="/etc /home /var/backups /var/lib /var/log /var/mail /var/local /opt/
↪altridata."
```

It is also advisable to configure a mail address to which emails with backup notifications will be sent, either by setting up an appropriate alias for the `root` user or by indicating a list of recipients (always separated by spaces) in the `MAILTO` variable, for example:

```
MAILTO="root localsysadmin@fuss.bz.it"
```

Finally if you want to maintain a more consistent history you can increase the value of the `RETENTION` variable that indicates the minimum number of backups maintained (in the maximum number of one per day, in case more than one backup is performed in the same day only the most recent one will be maintained). Keep in mind that `borg` supports deduplication, and that there is no concept of incremental backup; each backup is always complete.

3.5.3 Exclusion

Files that match the `fuss-backup.exclude` file (installed by default to exclude MPT, AVI, and ISO images) are not included in the backup. If the file is absent, the backup is performed without excluding anything.

In its most basic form, the format of the exclusion file involves one shell pattern (ex. `*.iso`) per line; files whose pathname matches the pattern are excluded. For more details (and examples of more complex patterns using regular expressions) refer to the documentation obtainable with the `borg help patterns` command.

The default installed by the package is to exclude from backups certain types of files (identified by exten- sion, particularly `*.iso`, `*.mp3`, and `*.avi`, and all `.cache` directories, which by containing a large amount of files can make backup execution very slow.

If necessary the program can be interrupted, what is saved by `borgbackup` until the last checkpoint (by default they are every half hour) will not be lost.

3.5.4 Restoration

Restoration can be done manually by mounting the disk (or the directory shared via NFS on the NAS) that contains the backup repository, and using the `borg` command to directly retrieve files from one of the backups. Read the documentation of the commands `borg list` (to list available backups) and `borg extract` (to extract data) with examples if you want to use this route.

To simplify operations, the `fuss-backup command` can be used interactively with the `fuss-backup mount` and `fuss-backup umount` commands to mount and unmount the backup data so that it can be accessed directly through the filesystem.

With `fuss-backup` mount the disk (or NFS directory) containing the data repository is mounted according to when configured in the `BASEDIR` variable (the default is `/mnt/backup`) and then the contents of the backups are made available via FUSE in the directory configured by the `RECOVERDIR` variable (the default is `/mnt/recover`). This allows direct access to the files in the backup made available through as many directories present under `/mnt/recover` in the form `fuss-server-DATE-TIME` (date and time refer to the time the backup was run), for example you may have something like:

```
root@fuss-server:~# ls /mnt/recover/ -l
total 0
drwxr-xr-x 1 root root 0 Jan 25 09:48 fuss-server-2017-01-20T17:39:56
drwxr-xr-x 1 root root 0 Jan 25 09:48 fuss-server-2017-01-25T09:40:51
```

so if you want to retrieve the files from the January 20 backup you will have to look for the fi- le under `fuss-server-2017-01-20T17:39:56` while for those from the 25th you will have to look under `fuss-server-2017-01-25T09:40:51`.

Below each directory will then appear the tree of directories that were covered by the backup according to the value of the `PATHS` variable. The directory tree is brought back from the root so in the case of the default values of `PATHS` illustrated above, we will have under `fuss-server-2017-01-25T09:40:51` the directories `etc`, `home` and `var`. A t this point you can copy/examine the files from the backup by browsing the filesystem under `/mnt/recover` with any file management tool.

Once the recovery operations have been completed, the directories and data must be unmounted, with the command `fuss-server umount`.

Warning: always remember to run the `fuss-backup umount` command, otherwise the ordinary execution of backups will fail.

3.6 Cleaning of Home

Fuss-server sets up a nightly home-cleanup cronjob, every night at 10 p.m., which performs a home cleanup, deleting files:

```
.config/xfce4/xfconf/xfce-perchannel-xml/displays.xml
.cache/chromium/*
.cache/google-chrome/*
.cache/mozilla/firefox/*
```

of all LDAP users except `admin` and `nobody`, and ignoring local users.

Starting with version 10.0.33, the time of this cronjob is editable via variables in `/etc/ fuss-server/fuss-server-defaults.yaml`:

```
home_cleanup_time_hour: 22
home_cleanup_time_minute: 0
```

3.7 Modifications of netmask

On a configured fuss-server, it is possible to change the netmask of the internal network: first change the network configuration in `/etc/network/interfaces` or `/etc/network/interfaces.d/`, setting the new netmask, and reload the new settings by, for example, restarting the server.

Tip: The network configuration can also be reloaded by `service networking restart` or with ifupdown2 (available in the debian repositories but not preinstalled on the fuss-server).

Then you can change the configuration in `/etc/fuss-server/fuss-server.yaml` and run `fuss-server create` to reapply the network configuration wherever it is needed.

Note: In case the addresses intended for DHCP are not included in the selected netmask, fuss-server will request a new range at the beginning of the run.

3.8 Troubleshooting - Troubleshooting problems.

3.8.1 Fuss-server administrative password reset

Change root password

To change the root password of the fuss-server, no special procedure is required; simply run the `passwd` command from `root`.

General service password change (master password)

The situation is more complex if, on the other hand, you want to change the "master password" that you used when creating the server (the one that is kept in the `pass` variable of the `/etc/fuss-server/fuss-server.yaml`).

In this case, there are many operations to be performed, as it is used extensively in the configuration of all services, so a special management script (`mpwchange.sh`, installed like the other scripts in `/usr/share/fuss-server/scripts`) has been provided to perform them at once.

To make the change, simply perform:

```
/usr/share/fuss-server/scripts/mpwchange.sh old_password new_password
```

the script checks in `/etc/fuss-server/fuss-server.yaml` that the old password matches and then changes it for the various services (and in `/etc/fuss-server/fuss-server.yaml` itself).

Should the command give an error, you can perform the individual steps manually as below:

1. "Prepare" the following command making sure to correctly fill in the following 5 fields containing the data of that specific school and the new password:

```
ldappasswd -v -x -h 127.0.0.1 -D "cn=admin,dc=___,dc=___" -W -A -s "_New-.
↪PASSWORD_""cn=admin,_dc=_,_dc= "
```

Fields to be filled in (5):

```
* dc= *1* (ex.appian)
* dc= *2* (ex.blz)
* "_NEW-PASSWORD_" (where the new password remains within the
↪virgolette " ")
```

(continues on next page)

(continued from previous page)

```
* dc= *3* (ex.appian)
* dc= *4* (ex.blz)
```

Example:

```
"_NEW-PASSWORD_"= MOON.69
```

The command to run is in the example:

```
ldappasswd -v -x -h 127.0.0.1 -D "cn=admin,dc=appiano,dc=blz" -W -A -s "LUNA.69
→""cn=admin,dc=appiano,dc=blz"
```

2. N.B.: Only the `old-password` is requested (3 times), as the `new password` is "passed" already from the command by the parameter `-s`

```
* Enter LDAP Password:              *(old-password)
* Re-enter old password:            *(old-password)
* Enter LDAP Password:              *(old-password)
```

The operation will have ended successfully if the following OUTPUT is returned.

```
Result: Success (0)
```

3. Edit the following files, replacing the `old-password` with the `new-password`.

```
vim /root/.ldapvirc
```

4. Run the following command followed by the new password instead of the field _____:

```
smbpasswd -w _____
```

Output like the following will be returned:

```
Setting stored password for "cn=admin,dc=appiano,dc=blz" in secrets.tdb
```

5. Edit the following files, replacing (2 times) the `old-password` with the `new-password` .

```
vim /etc/smbldap-tools/smbldap_bind.conf
```

6. Run the following command and enter (2 times) the `new-password`:

```
/usr/sbin/smbldap-passwd admin
```

```
Changing UNIX and samba passwords for admin
* New password: _____
* Retype new password:_____
```

7. Edit the following file by replacing the `password`:

```
vim /etc/octofuss/octofuss.conf
```

8. Restart the service:

```
service octofussd restart
```

9. a. Run the following command followed by the new password instead of the field _____

```
octofussd --reset-root-password _____
```

Output like the following will be returned:

```
System check identified some issues:
WARNINGS:
?: (1_7.W001) MIDDLEWARE_CLASSES is not set.
HINT: Django 1.7 changed the global defaults for the MIDDLEWARE_CLASSES.␣
↪django.contrib.sessions.middleware.SessionMiddleware, django.contrib.
↪auth.middleware.AuthenticationMiddleware, and django.contrib.messages.
↪middleware.MessageMiddleware were removed from the defaults. If your␣
↪project needs these middleware then you should configure this setting.
Operations to perform:
Apply all migrations: data
Running migrations:
No migrations to apply.
```

b. Run the following command (WARNING: kerberos "interactive" mode!):

```
kadmin.local
```

CAUTION: You enter an "interactive" mode of kerberos and the following line will be displayed:

```
kadmin.local:
```

c. after which you will need to copy the following command:

```
cpw root/admin
```

Eventually the following line should be displayed on the terminal:

```
kadmin.local: cpw root/admin
```

d. Press the ENTER key: you will be asked 2 times for the new password:

```
* Enter password for principal ``root/admin@APPIANO.BLZ`` : _____________
* Re-enter password for principal ``root/admin@APPIANO.BLZ`` : _____________
```

screen then the following prompt opens:

```
kadmin.local:
```

e. Exit this interactive mode by typing:

```
exit
```

10. Edit the following file to replace the `MASTER-PASSWORD`:

```
vim /etc/fuss-server/fuss-server.yaml
```

Recommended optional procedures

1. If you want the `master password` to match `the root password`, update it as well:

```
passwd root

New password:_____________

Re-enter the new password: _____________
```

2. You can then go into the history and delete the traces of the commands containing the new password. The procedure is as follows:

    1. Display the list of commands and their `sequence number` by launching the command:

```
history
```

2. Delete the specific command (say it is number 764 in the list) with:

```
history -d 764
```

3. Confirm the changes with:

```
history -w
```

3. At this point possibly upgrade the server.

3.8.2 Restoring LDAP from a backup

The `fuss-backup` package backup script (see *Backup with fuss-backup*) takes care of dumping the LDAP directory data, we will now see what is the procedure for its restoration.

LDAP database dumps are saved by `fuss-backup` in `/var/backups/slapd` at each run (deleting older ones) in `gzip-compressed` files in the form `slapd-$DATA.ldif.gz*`, but you can also generate them at any time with the command `slapcat > backup.ldif`.

It is preferable to restore server data from a dump generated with `slapcat` because this contains all the information in the original LDAP (including metadata, such as timestamps of various changes). The restoration procedure is as follows:

```
systemctl stop slapd.service
rm -rf /var/lib/ldap/*
slapadd < backup.ldif
chown openldap:openldap /var/lib/ldap/*
systemctl start slapd.service
```

(where backup.`ldif` is the backup file, if using one of the `fuss-backup` dumps this must first be unzipped).

3.8.3 LDAP Troubleshooting

User does not login to Windows

Trivial things to check first:

- does the user exist?
- Has the join to the domain been done correctly?
- domain and host name are correct?
- capslock?
- network cable? :-)

It could at this point be a problem with LDAP, or rather how the user was created/modified on LDAP If windows tells you that the user is disabled, the `sambaAcctFlags` record is probably not set correctly. The D flag indicates that the user is disabled, a user should normally report the U flag or at most the UX flags

To correct the situation use the command:

```
smbldap-usermod -H U username
```

or you use `ldapvi`

In case there are many users to be migrated, one can create a teachers.`txt` file containing the list of teachers' user names, one per line, and then use the command:

```
for user in $(cat docenti.txt); do smbldap-usermod -H U $user; done
```

3.8.4 DNS Troubleshooting

Failure to resolve reinstalled machines with the same name

The fuss-server uses dynamic DNS to automatically create entries with the names of the machines within the school's local zone, with the `standard ddns-update-style` directive in `/etc/dhcp/dhcpd.conf`. The mechanism requires that whenever a client obtains a dynamic address from DHCP, an entry with its name (which is invited by the client itself, and corresponds to its hostname) is placed within the local zone and the reverse zone of DNS so that it can refer to it directly by name.

The data are entered into the file `/var/cache/bind/db.local`, which contains the data of the DNS zone used for the school's internal network (those of the internal resolution in `/var/cache/bind/db.192.168.XX.YY` depending on the assigned address range), where entries will appear in the form:

```
test-client                A       192.168.13.57
                           DHCID   (
                                   AAIBP7QJ7mJsQfNKCJli4K991QOr0lDOCeqRUWvz1A1U
                                   SUE= ) ; 2 1 32
```

The entry consists of the assigned IP and a `DHCID` field, which is an identifying hash of the client (usually hostname and MAC address, but it depends on the client itself) that is used to prevent another machine from trying to sneak into DNS assuming the same name and to prevent two machines assigned (incorrectly) the same name from overwriting each other's entry on DNS.

These records are usually deleted automatically when the client releases the IP, but it may happen, when this does not happen properly (e.g., because it is shut down without shutdown), that they remain in the file. They are usually not a problem until you reinstall a client with the same name, which will have a different DHCID so it will not be able to reuse the name or remove the entry.

A contingency solution may be to add to `/etc/dhcp/dhcpd.conf` the direct- va `update-conflict-detection no` immediately below the previous `standard ddns-update-style`, this allows for rewriting, but results in the conflict checks no longer being there, and you will get situations where problems, manifesting themselves in a random form, are much more difficult to diagnose and recognize. Therefore, it is an emergency solution that should never be used for more than the narrow time needed to solve an immediate problem; the correct solution is to remove the records that give the problem, with the procedure outlined below.

Removal requires manual editing of the zone files mentioned above (`/var/cache/bind/db. local` and `/var/cache/bind/db.192.168.XX.00`), but since the assignment is dynamic, the contents of these files may not necessarily be updated to the current situation (temporary data are kept in binary form in corresponding `.jnl` files), and in addition, the data may further updated during the change, so before starting it is necessary to "freeze" the situation with the command:

```
rndc freeze
```

which saves all temporary data and blocks DNS updates by DHCP.

You can then look inside `/var/cache/bind/db.local` for dynamic entries to remove similar to the one illustrated. Keep in mind that in some cases these are introduced by a line like:

```
$TTL 3600       ; 1 hour
```

which indicates the lifetime of the entries listed below (the value shown may be different depending on the settings given to the DHCP server). This value is set, as often as it varies, at the beginning of a block of entries and applies until the next reset, so it can help identify dynamic entries

compared to the static ones set when creating the file with the fuss server installation, which have a value of `604800`.

When removing an entry take care to remove it only when it is unnecessarily replicated. If you decide to do a complete cleanup of all dynamic entries it should be removed preventing it from applying to the remaining static entries. In general, deleting all entries related to dynamic assignments is not a problem (they will be recreated at renewal or next request) but the resolution of deleted names will obviously become unavailable until then. Therefore, it is recommended to delete only those entries containing the problematic names.

Also be careful not to delete or modify instead the "fixed" entries in the file, such as the names `ns`, `proxy`, `octofuss`, etc., and in general all those that you have manually entered in the file for static assignments.

Once you have removed the entries from `/var/cache/bind/db.local` delete the corresponding entries with the reverse rice- luation in `/var/cache/bind/db.192.168.XX.00`, which in the case of the previous example will be something like:

```
57                      PTR     test-client.fusslab.blz.
```

Once the changes have been completed, the serial of the zone files (both of them) must be updated; for this you need to look for the line identified by the comment `; serial` in the `SOA` record that is at the beginning of the file, and increase the value in it by one; if, for example, 811 was the value in `/var/cache/bind/db.local` prior to the changes, you will have to indicate 812 instead, with something like:

```
$ORIGIN .
$TTL 604800     ; 1 week
fusslab.blz             IN SOA ns.fusslab.blz. root.marcela.fusslab.blz. (

                                812         ; serial
                                604800      ; refresh (1 week)
                                86400       ; retry (1 day)
                                2419200     ; expire (4 weeks)
                                604800      ; minimum (1 week)
                                )
```

When this is done, you can "unfreeze" the area with the command:

```
rndc thaw
```

and dynamic updating will resume.

Failure to resolve statically assigned machines

One of the features provided by the fuss-server is to allow static assignments (re- servation) of IPs based on the MAC address of the machines. These are maintained in the `/etc/dhcp/dhcp-reservations` and managed through `octonet`.

`Until` version 10.0.13 `octofussd` merely handled this static assignment, the machines listed in the file were not entered into DNS. Therefore, the listed machines get an IP address (the one selected by the feature) but their name remains absent from DNS.

As of version 10.0.14, support has been added for insertion (when creating) and deletion (when removing) on the DNS of machines indicated for static assignment. Support for editing data is not yet available (so delete and recreate an entry if needed).

However, the support available as of version 10.0.14 is only for new entries; for existing entries, DNS is not updated. To handle this case (or if you are maintaining use of a version prior to 10.0.14) entries must be inserted or deleted by hand.

The operation involves manually modifying the zone files (`/var/cache/bind/db.local` and `/var/cache/ bind/db.192.168.XX.00`), which are dynamically managed; for this (review what has already been said about this in the previous section, before modifying them, it is necessary to "freeze" the situation with the command:

```
rndc freeze
```

at this point the data can be added, in `/var/cache/bind/db.local` the direct resolution should be put, using a suitable TTL, with something like:

```
$TTL 604800     ; 1 week
static1             A       192.168.0.100
```

(taking care to use the name and address that are there in `/etc/dhcp/dhcp-reservations`) where the TTL entry can be omitted if the line is inserted under a definition block that has it at the beginning.

The change should also be made in the reverse zone (in `/var/cache/bind/db.192.168.XX.00`) with something like:

```
$TTL 604800     ; 1 week
100                     PTR     static1.fusslab.blz.
```

and the same warning applies with respect to TTL, having made the changes you will need to increase the serial again (refer to what was said in the previous section) and then you can "unfreeze" the zone with the command:

```
rndc thaw
```

resolutions will be available at this point.

Starting with `fuss-server` 10.0.24, the `dnsreserv.py` script is available (in `/usr/share/ fuss-server/scripts`) that rereads the contents of `/etc/dhcp/dhcp-reservations` and performs a DDNS update for all the names contained therein; this avoids manual intervention to reinstate them, but the possible deletion of spurious names is not performed, and in that case the previous manual procedure must be used.

3.8.5 Corruption of the backup repository

It may happen that, if the program is interrupted inappropriately, the repository that keeps the backup data will be corrupted. In such a case you may get errors (reported in the summary email sent at the completion of each backup) such as:

```
borg.helpers.IntegrityError: Segment entry checksum mismatch [...].
```

In this case it is necessary to perform a manual verification, and possibly repair the data repository.

To do this you need to mount the remote disk to which you make backups, this can be done (using the data contained in the fuss-backup configuration) with the commands:

```
. /etc/fuss-backup/fuss-
backup.conf mount $DISK $BASEDIR
```

Then you can check the status of the repository, with:

```
borg check $BASEDIR/$BACKUP_DIR
```

And if this reports errors they can be fixed with:

```
borg check --repair $BASEDIR/$BACKUP_DIR
```

accepting that you may lose data (this is backup data, you can restore it by doing one immediately after the repair). Once the repair is complete, remember to unmount the remote disk with `umount $BASEDIR`.

CHAPTER 4

FUSS client management

4.1 Configuring a *FUSS Client*

To configure a machine as a *FUSS Client,* the `fuss-client` command is available, installed with the pacchet of the same name, which takes care of all the configuration of the machine, and the eventual connection of the machine to the *Fuss Server*, installing the necessary software and making the relevant configurations.

4.1.1 Ordinary installation

The main command for configuring the client is `fuss-client -a`, which connects to a *Fuss Server* automatically detected in the network where the machine was plugged in.

If you have a flash drive with an authentication key for the *Fuss Server* this must be inserted on the machine, and the procedure will be fully automated (for details see *Keyed Access to the server for fuss-client*), otherwise once the command has been launched the *Fuss Server* root password must be entered three times to allow the necessary credentials to be imported.

If there are no clusters defined on the *Fuss Server it* **is necessary to** define one in advance, if only one is defined nothing else will be asked and the installation will continue directly to the end, obtaining on the terminal a result like:

```
PLAY RECAP
********************************************************************* localhost
                              : ok=129 changed=71    unreachable=0    failed=0
```

(where you must have `failed=0`)

If, on the other hand, there are multiple clusters on the *Fuss Server* at the beginning you will be asked to choose in which one to be placed with a screen like:

```
This server has several workstation groups

Please choose the one desired for this machine:
0  - classroom1
1  - classroom2

Your choice? (enter the server number)
0
...
```

4.1.2 Hostname setting

The `fuss-client` command supports the installation and connection to the server of a machine with the con- textual setting of its name. This is useful when a pc is installed using an image created with clonezilla, which obviously has set the hostname of the client from which it was created.

In addition, the `fuss-client` command performs a normalization of machine names, in fact in some cases the full hostname (FQDN) of the machine was being used as the hostname of the machine, which then creates problems in name resolution and inserted the same in the `/etc/clusters` file of the server. This what had then led to using as the full hostname (set in `/etc/hosts`) a simple name with no domain (which could cause problems with any services installed later).

When installing and connecting a client to the server, the command that allows the contextual setting of the machine hostname using the `-H` option in the form:

```
fuss-server -a -H clientname
```

where clientname must be an alphanumeric domain name that must **not** contain any ".", and be indicated only by lowercase letters.

In this case, the client, having obtained the domain name from the server, will make the correct setting of the `/etc/ hostname` files, simply entering the given name with content such as:

```
clientname
```

while in `/etc/hosts` the correct value for full resolution with content such as:

```
127.0.1.1       clientname.institute.lan clientname
```

And it will be correctly obtained that:

```
root@testclient:~# hostname
clientname
root@testclient:~# hostname -f
clientname.institute.lan
```

and in this way in the server's `/etc/clusters` file the machine name will be used.

4.1.3 Veyon

Starting with FUSS Client 10.0.40, configuration of Veyon is done fully automatically by extracting data on clients from `/etc/clusters` on the FUSS server.

Only users belonging to the
`veyon-master group` (which should therefore be appropriately chosen and associated with the group).

For security reasons, controls have been implemented to ensure that no user who is a member of at least one of the following groups can be controlled by anyone else through Veyon

```
- faculty
- teachers
- veyon-master
- technicians
```

Should you wish to inhibit additional groups, you will need to create the text file `/var/www/html/veyon/excluded_groups` with, one per line, the names of the groups.

Please note: this file also allows overriding of pre-set groups, which should therefore be placed in the `excluded_groups` file to avoid, for example, control over the faculty group.

Several features of Veyon such as turning PCs on and off, sharing the teacher's screen, or updating PCs are not currently usable and will be hidden from the interface with an upcoming update.

4.2 Updates

4.2.1 Minor updates to fuss-client

In case there are minor version updates of fuss-client (10.0.x → 10.0.(x+1)) you can apply them by updating the package:

```
# apt update
# apt install fuss-client
```

and then launching:

```
# fuss-client -U
```

To apply the new configurations.

The information in `/usr/share/doc/fuss-client/changelog.gz` (after package installation) can be useful to find out if the changes are useful for existing installations or if they affect only new installations.

4.3 Keyed server access for fuss- client

In order to connect clients to a fuss-server, it is necessary to give ssh access to the server to the person making the connection; it is possible to restrict this access by using a special ssh key that gives root access to the server, limited, however, to only the commands necessary for `fuss-clients`.

With the `fuss-server create` or `fuss-server upgrade` commands, a key pair is created in `/etc/fuss-server/client_keys/client-rsa(.pub)` and it is enabled for `fuss-client` to access the server.

On clients already configured with `fuss-client`, there is a script, `/usr/local/sbin/copy_server_key`, that prepares a USB stick configured to be recognized by `fuss-client`, which then mounts it, uses it for identification, and then unmounts it when no longer needed, so that it can be moved to other clients.

Alternatively, you can transfer the private key to clients in any other way you like and use the `-k` option `</path/complete/key>` to identify without a password. In this case it is, of course, the user's responsibility to mount and umount any removable devices.

Note: ssh requires that the key file have permissions such that other users cannot read it; if such files are on ext filesystems, it is appropriate to assign permissions `0600` to the private key file.

If a FAT filesystem is used instead, appropriate mount options must be used to prevent files from showing up with `0755` permissions, which is the default.

In both cases, the files on the flash drive are used during the initial fuss-client phase; when they are no longer in use, a different sound is made depending on whether the flash drive has been disassembled and you can safely remove it or there have been problems in disassembly and so you can disassemble it by hand and remove it.

In case you do not hear the sound, it occurs just before the moment when the colored ansible lettering begins.

4.3.1 Key Management

Adding new keys on the server

You can enable new keys by putting the public and private key pair in `/etc/fuss-server/client_keys/` and running `fuss-server upgrade` for them to be enabled for access.

`/etc/fuss-server/client_keys/client-rsa(.pub)` must exist (otherwise a new one is created) and is the default key used for example by the `copy_server_key` script, other keys must be managed manually.

Disabling keys

Disabling a key from the server requires:

- remove the corresponding line from `/root/.ssh/authorized_keys`
- Remove public and private keys from `/etc/fuss-server/client_keys/`

Creating a USB flash drive with ssh keys

On already configured clients, starting with version 9.0.16 of fuss-client, there is a script, `/usr/local/sbin/copy_server_key`, to create USB sticks containing ssh keys to be used for identification. The script does not depend on other fuss-client components and can be copied to other machines, in which case you must have installed the `python3-pyudev` package (a dependency of `fuss-client`) to use it.

To use it, connect an empty USB flash drive to the computer and run the command:

```
# copy_server_key /dev/sdXn
```

where `/dev/sdXn` is the device corresponding to the partition on the stick where you want to save the keys.

Warning: The specified partition will be reformatted, losing any data that may be on the flash drive.

By default, the key present on the server reachable at the `proxy` address is copied; alternatively, the server address can be specified via the `-s <address.of.server>` option.

Warning: In the version of mkfs.ext4 found in Debian Buster, and thus on the older fuss-clients, there is a bug in the Italian localization, #907034, that prints confirmation requests in English, but expects response in Italian.

If a request like:

```
mke2fs 1.43.4 (31-Jan-2017)
/dev/sdb1 contains an ext4 file system labeled "keychain" last
    mounted on /mnt/keychain on Mon Aug 13 09:40:52 2018
Proceed anyway? (y,N)
```

you must press `s` to continue; `y` is not recognized and is treated as the default, `n`, which then causes immediate exit from the program.

4.3.2 Specifications

USB keys for ssh key distribution

In order to work securely, `fuss-client` without the `-k` option requires that ssh keys be saved on a precisely configured USB stick, as generated by the `copy_server_key` script.

The USB flash drive must contain an ext formatted partition with a `keyring` label, within which is a `server_key` directory containing the `client-rsa` file with permissions `0700` and `0600`, respectively, both belonging to the `root` user.

4.4 Troubleshooting problems

4.4.1 Diagnosis of fuss-client errors

In order to troubleshoot any problems with the installation of a client during the execution of `fuss-client`, it is essential to have the complete log of the operations performed by *ansible* during execution; reporting only the final result lines is not sufficient.

Therefore, in case problems occur, it is advisable to relaunch the command by following the directions for recording the session outlined in *Bug reporting*.

4.5 Procedures alternatives

4.5.1 Installation on Debian 12 (bookworm)

Fuss Client can be installed on a standard Debian 12 (bookworm); in that case, some configuration needs to be done, again working as root.

- Install Debian 12 (bookworm) by retrieving one of the following ISOs (as needed):

Architect-ture	ISO xfce-desktop UFFICIA-. THE	UNOFFICIAL xfce-desktop ISO (with firmware owners)
amd64	debian-live-<version>-amd64-xfce.iso	debian-live-<version>-amd64-xfce+nonfree.iso
i386	debian-live-<version>-i386-xfce.iso	debian-live-<version>-i386-xfce+nonfree.iso

- Enable fuss repositories in `/etc/apt/source.list.d/archive_fuss_bz_en.list`:

```
deb [signed-by=/usr/share/keyrings/fuss-keyring.gpg] http://archive.fuss.bz.it/
↪bookworm main
```

- Add the repository signing key and update apt:

```
# wget -qO /usr/share/keyrings/fuss-keyring.gpg https://archive.fuss.bz.it/
↪apt.gpg
# apt update
```

- And finally, run the fuss-client program:

```
# fuss-client -a
```

4.5.2 Standalone installation

fuss-client also supports a standalone installation mode that does not connect to a fuss-server, but merely configures a debian installation with the programs and customizations of the fuss system.

To use it, starting with a clean installation of Debian, simply add the fuss repositories in `/etc/apt/source.list.d/archive_fuss_bz_en.list`:

```
deb [signed-by=/usr/share/keyrings/fuss-keyring.gpg] http://archive.fuss.bz.it/ ␣
↪bookworm main
```

- Add the repository signing key and update apt:

```
# wget -qO - https://archive.fuss.bz.it/apt.key | gpg --dearmour > /usr/share/
↪keyrings/fuss-keyring.gpg
# apt update
```

- And finally, run the fuss-client program:

```
# fuss-client --standalone
```

Chroot configuration for iso generation

In case you are configuring with `--standalone` not a real machine but a chroot, you can add the `--iso` option toprevent grub and locales from being configured to avoid failures.

4.5.3 Light installation

The `--light` option makes it possible to do lighter installations by avoiding installing the inter metapackages `fuss-kids`, `fuss-children` and `fuss-education`. Of course, a more limited selection of educational packages can be installed manually at a later time.

4.5.4 Support for proprietary firmware

The operation of certain hardware requires the use of proprietary firmware, available in the `non-free-firmware` repositories.

The `--unofficial` option of `fuss-client` adds installation of such firmware; to use it, you must enable the `contrib`, `non-free-firmware`, and `non-free` sections for debian repositories in `/etc/apt/sources.list`.

Warning: As the name implies, this option is to be considered unofficial, and in particular the installation of software from `non-free` other than firmware required for hardware support is not supported.

4.5.5 Hostname change

To change the hostname of a fuss-client you can run the command:

```
fuss-client -H <new_hostname>.
```

this also updates the kerberos key with the new hostname.

The option is intended to be used on machines just restored from a clean image to assign a unique hostname to it immediately before configuring it with fuss-client.

The use of this option on machines already configured with fuss-client is adequate in the case where a mistake was made in assigning the hostname, but it is not recommended to make systematic use of it, and particularly in the case of changing the server it is advisable to restore from a clean image.

In case you use this option on a client that has already been connected to a fuss-server, it is also appropriate to use, on the server, the command:

```
/usr/share/fuss-server/scripts/forget_client <old_hostname>.
```

To remove traces of the registration with the previous hostname.

4.5.6 Complete removal of configuration

Once a client has been configured, its configuration cannot be reliably removed; to totally change a client's use case, it is necessary to restore its installation from a clean image via fuss-fucc (or perform a fresh installation, whichever is more convenient or faster).

Keeping the same use case, in some cases a re-configuration with the option
`--H` documented above and the new parameters, but there is no guarantee that it will work, and in any case it is not usable for switching from client to standalone systems and vice versa.

CHAPTER 5

The management interface of OctoNet

5.1 Architecture

5.1.1 Services necessary for operation

In order to use the *OctoNet* management interface, the entire *Octofuss* management infrastructure) provided by the *Fuss Server* must be active, which requires the following three services (managed with *systemd* and launched at server startup):

- **octofussd**: *Octofuss* management infrastructure daemon (verifiable with `systemctl status octofussd`);
- **octonet**: service that provides the web interface of *OctoNet* (verifiable with `systemctl status octonet`);
- **octofuss-client**: local machine control daemon, also to be installed on the server (verifiable with `systemctl status octofuss-client`).

5.1.2 Access to the web interface

The *Fuss Server* provides the *OctoNet* web-based management interface, which is accessed through a browser.

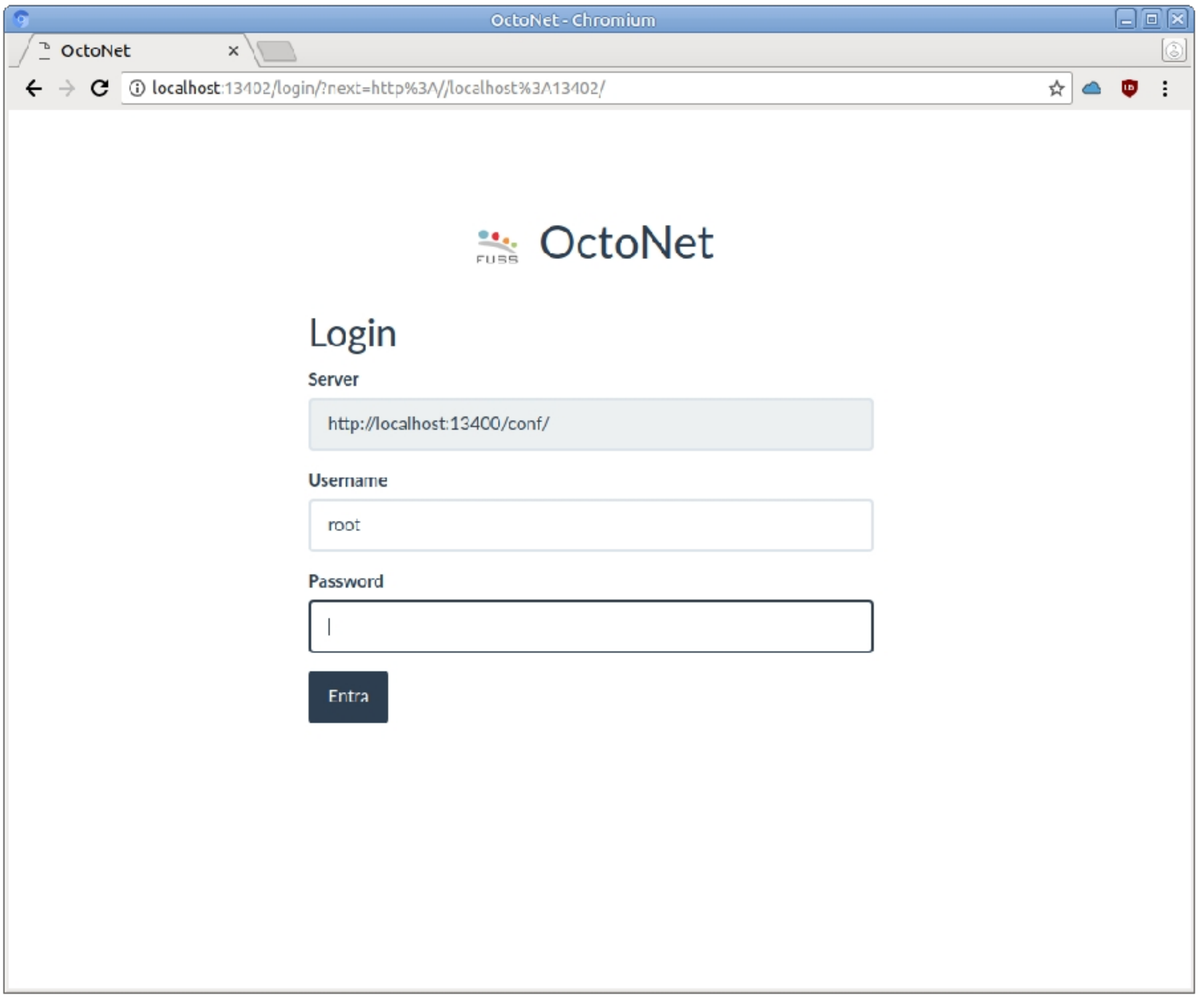
On the server itself you can log in using the address http://localhost:13402; since access is provided without encryption it is not safe to connect to it directly from other machines, but you can use an SSH tunnel: on a terminal from any client on the internal network run:

```
$ ssh sshuser@proxy -L 13402:localhost:13402
```

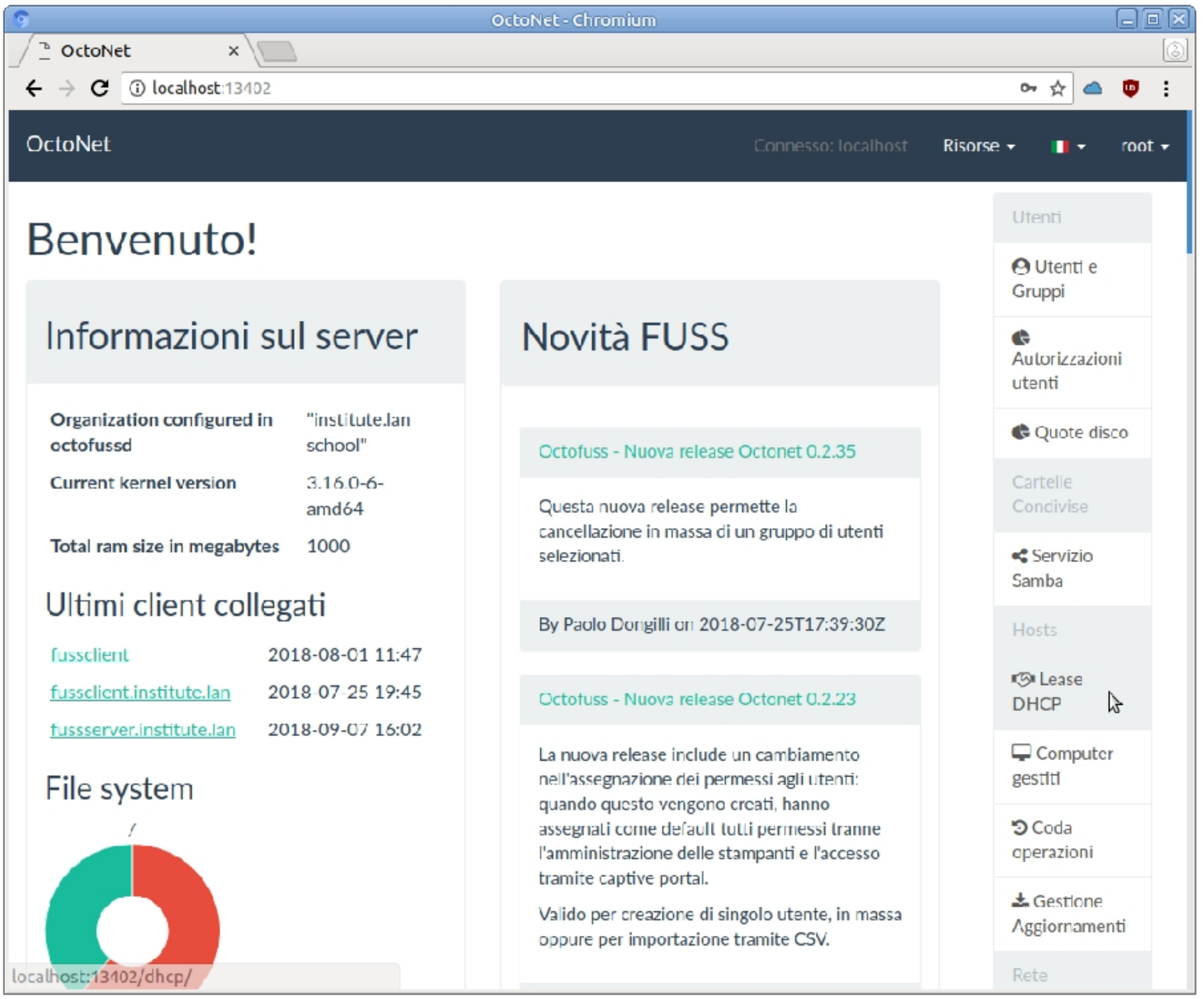
where `sshuser` is any user with SSH access on the server (i.e., part of the `sshaccess` group). To enable access to the new *Fuss Manager* platform as well, port `1232` must also be connected:

```
$ ssh sshuser@proxy -L 13402:localhost:13402 -L 1232:localhost:1232
```

Once connected in the console, the web interface can be accessed using a browser on the client by pointing it to http://localhost:13402, where you will get the following login screen:



With the installation of the *Fuss Server*, a default login is created with a `root` username and password equal to the master password set while running the `fuss-server create` command (the created user is internal to the `octofussd` service and has nothing to do with the system `root` user). Once logged in you will get a page like the following:



On the page, a menu of the different management features provided by OctoNet is available in the column on the left. Keep in mind that the menu is dynamic and shows the different features only when they are available (for example, if disk quotas have not been enabled, the relevant item will not be present).

The top bar shows a user menu to the right that allows disconnection, and to its left a language choice menu (English, Italian, and German are available). In what follows we will refer to the Italian version.

5.1.3 The command line interface octofussctl

The *Octofuss* infrastructure provides a command-line tool, `octofussctl`, which allows management operations to be performed in scriptable form.

The command requires the same login credentials used for *OctoNet*, and provides both an interactive command line and the ability to perform batch operations (writing the relevant commands within a text file to be passed to the command with the `-b` option).

The URL identifying the server, in the form, must be given for access:

```
octofussctl http://localhost:13400/conf
```

you can indicate the user with the `-u` option (or with the `OCTOFUSS_USER` environment variable) while the password, if not indicated in the `OCTOFUSS_PASSWORD` environment variable, is required on the terminal. The credentials are the same as those used for *OctoNet* (and the above applies).

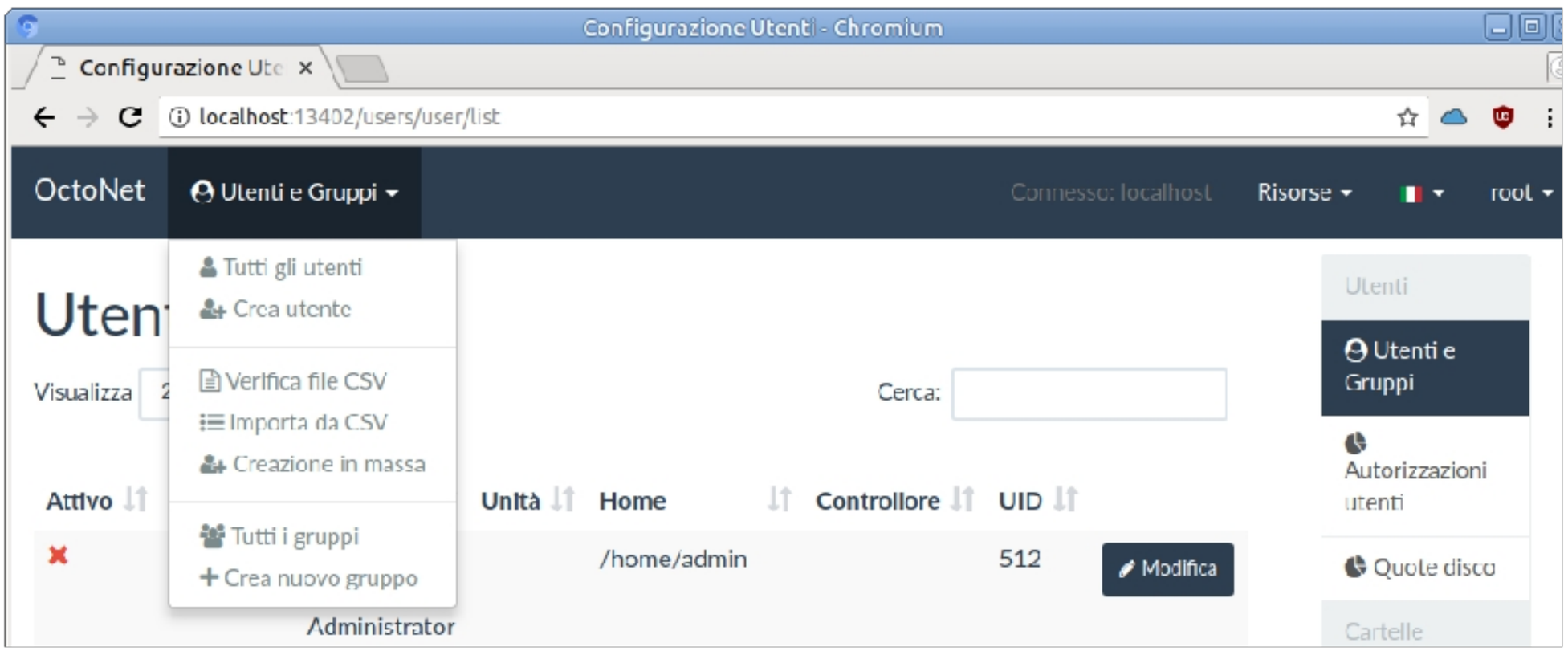
The commands available within the `octofussctl` shell are listed by the `help` command, and its operation by `help command`.

With `octofussctl it` becomes possible to automate some operations that would become very cumbersome to perform through the web interface; for example, if you wanted to delete all the users in a group (the web interface allows you to remove them from a group, but not delete them), you could use the `delete` command in a loop such as:

```
export
OCTOFUSS_PASSWORD=password
export OCTOFUSS_USER=root
for i in $(members group); do
  octofussctl http://localhost:13400/conf delete /users/users/$i
done
```

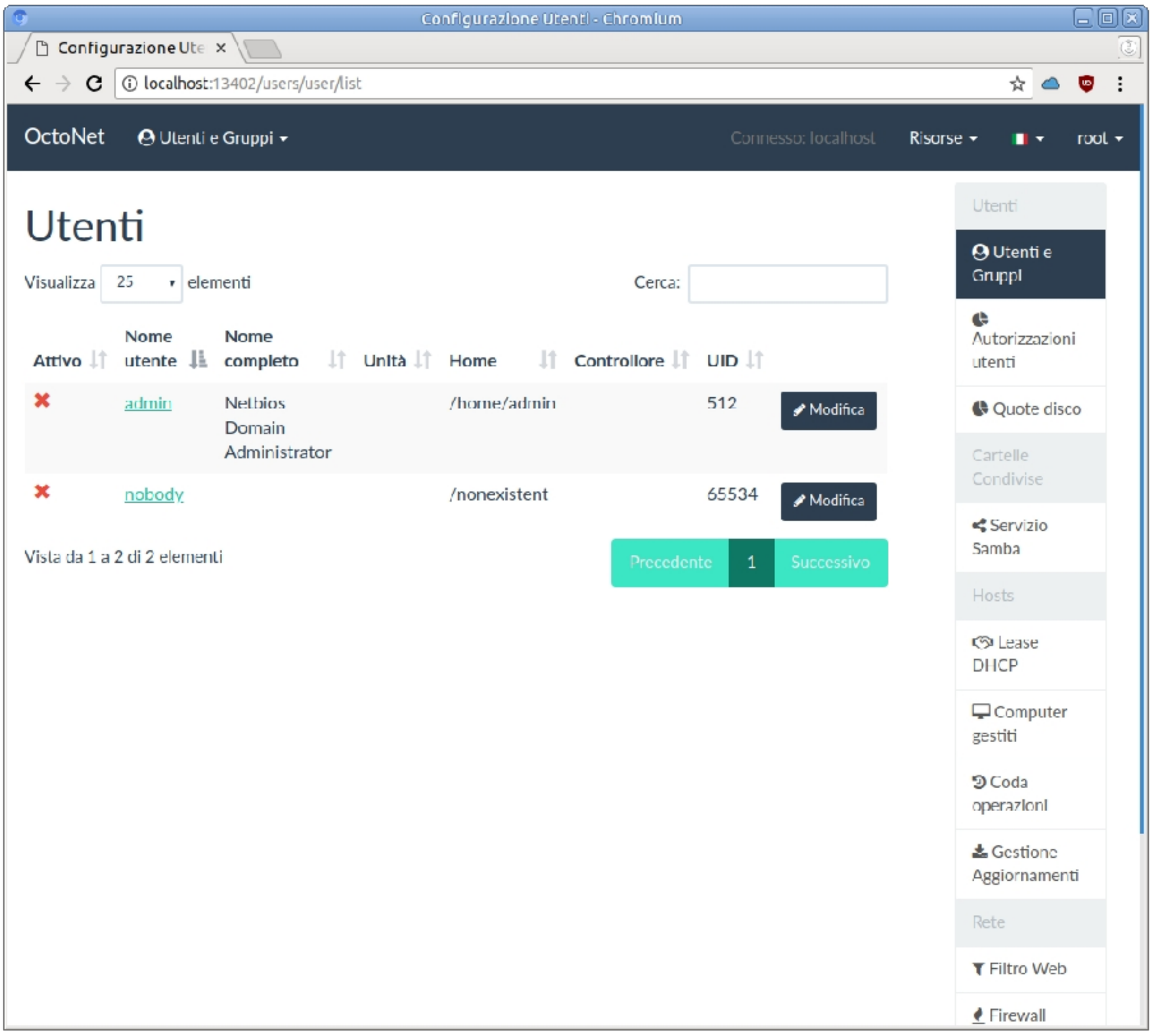
5.2 Managing Users and Groups

OctoNet user management can be accessed through the *Users and Groups* item, which enables on the top bar (on the left) a menu of the same name from which to access the other pages.



5.2.1 Viewing users

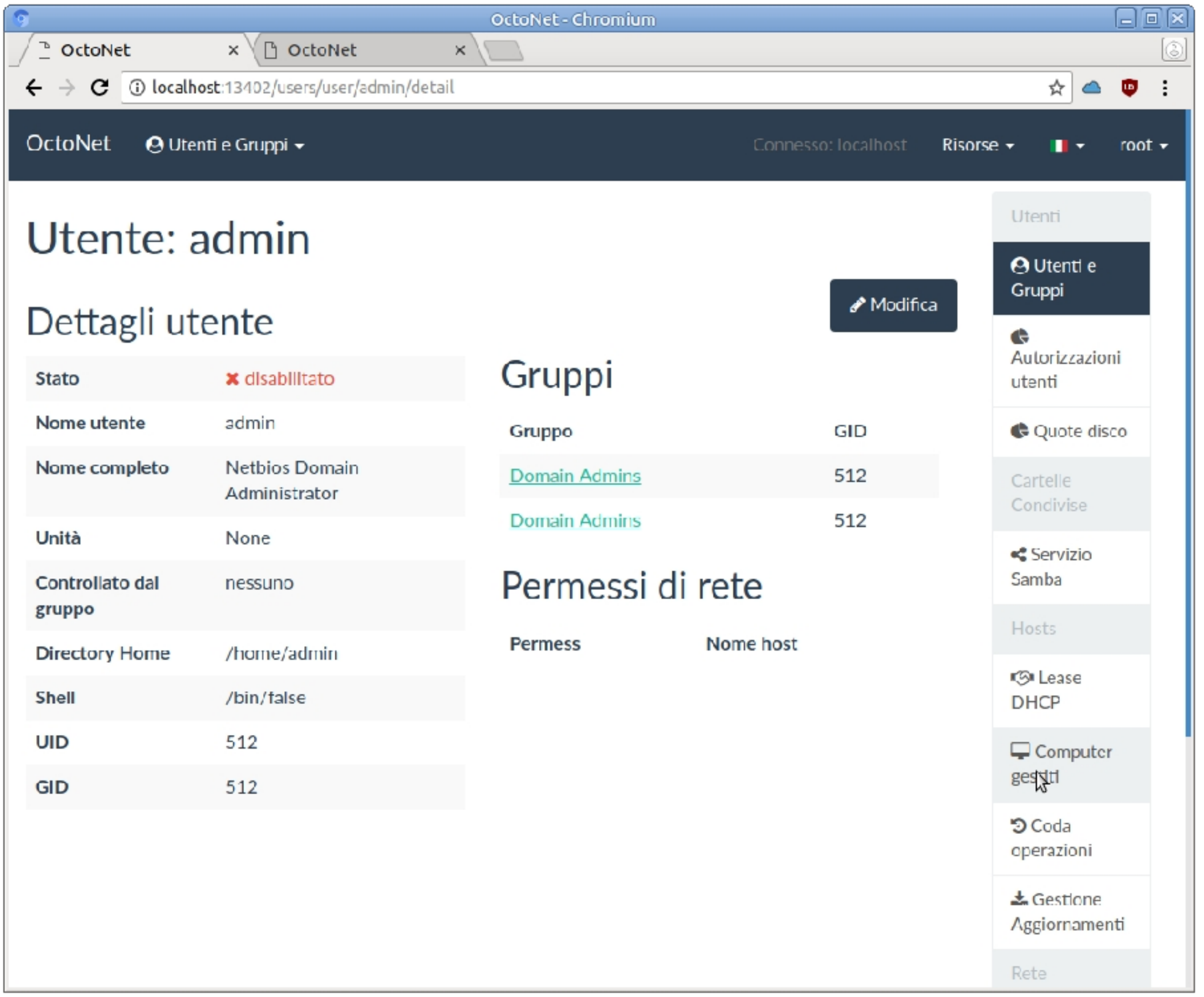
Once user management is selected you are taken to the user management page (corresponding to the *All Users* item in the above menu).



The page displays a table with all the users created on the server (only those centrally managed through the LDAP service), two of these, `admin` and `nobody` are ever-present service users that should not be changed (they are disabled, and therefore marked with a red cross).

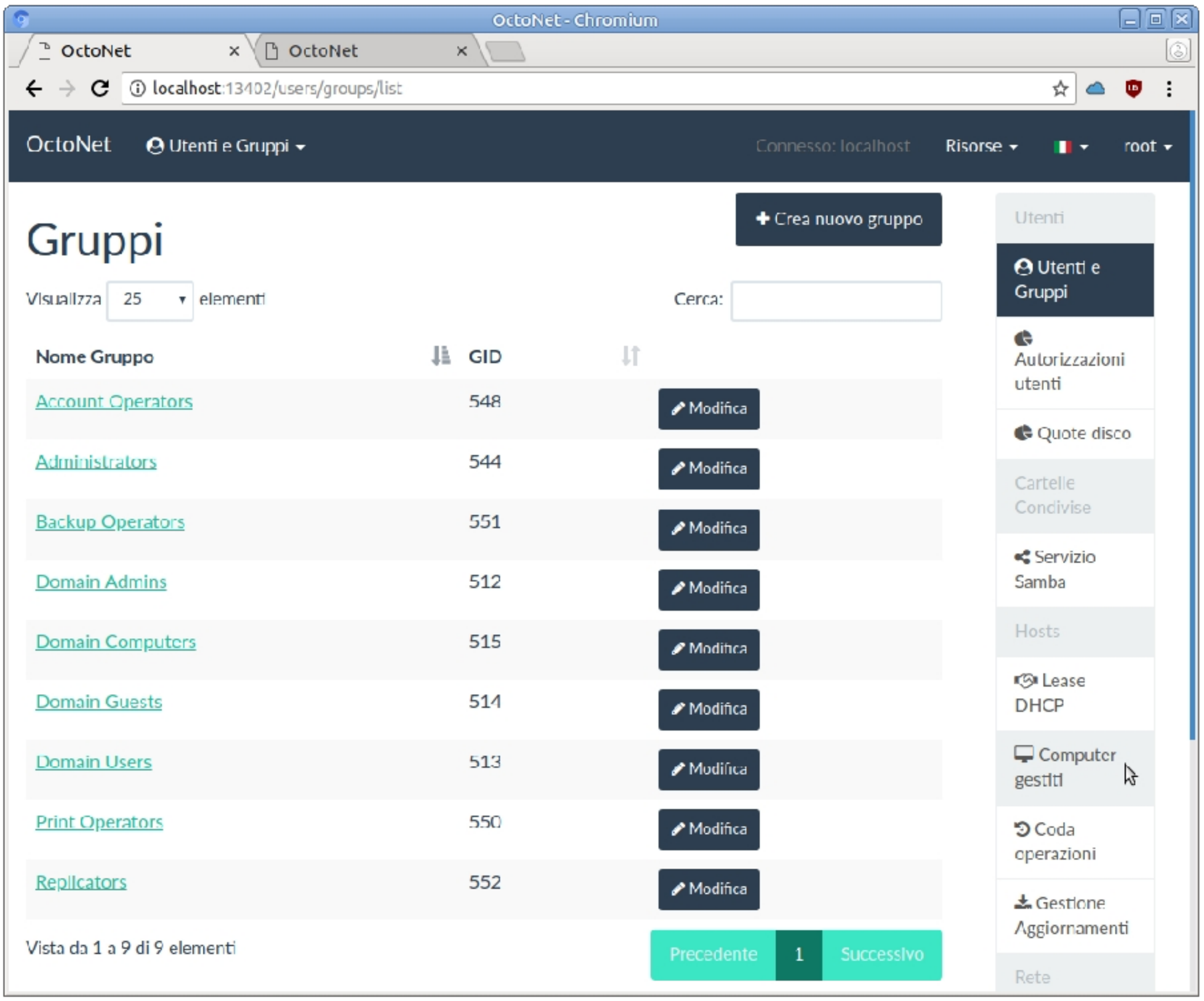
You can change the number of users displayed by selecting one of the options in the *View* drop-down menu on the left or perform a search on the user name by entering a string in the *Search* field.

Clicking on the link with the user's name in the second column or the edit button on the user's row will take you to the user's management page:

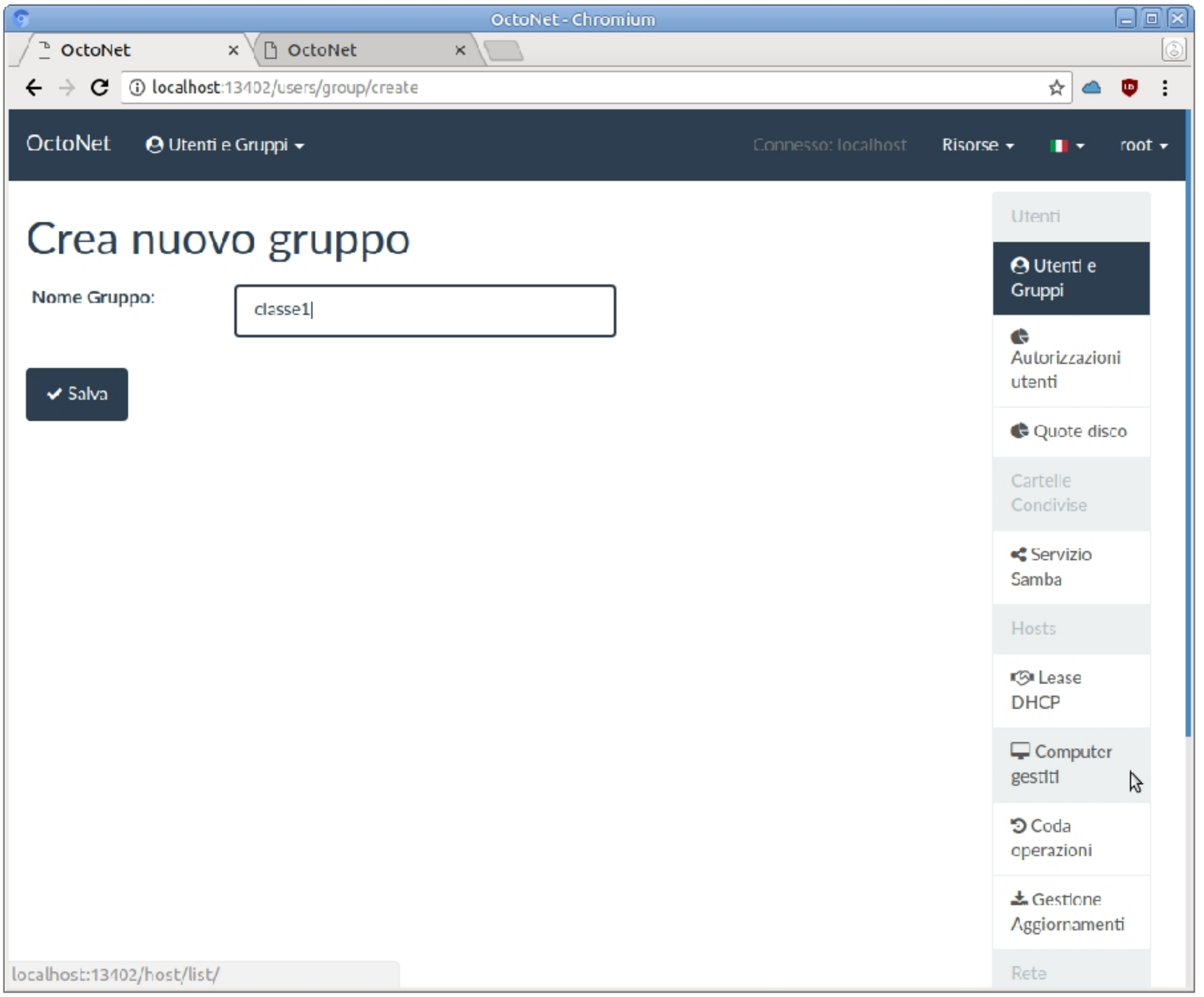


5.2.2 Group management

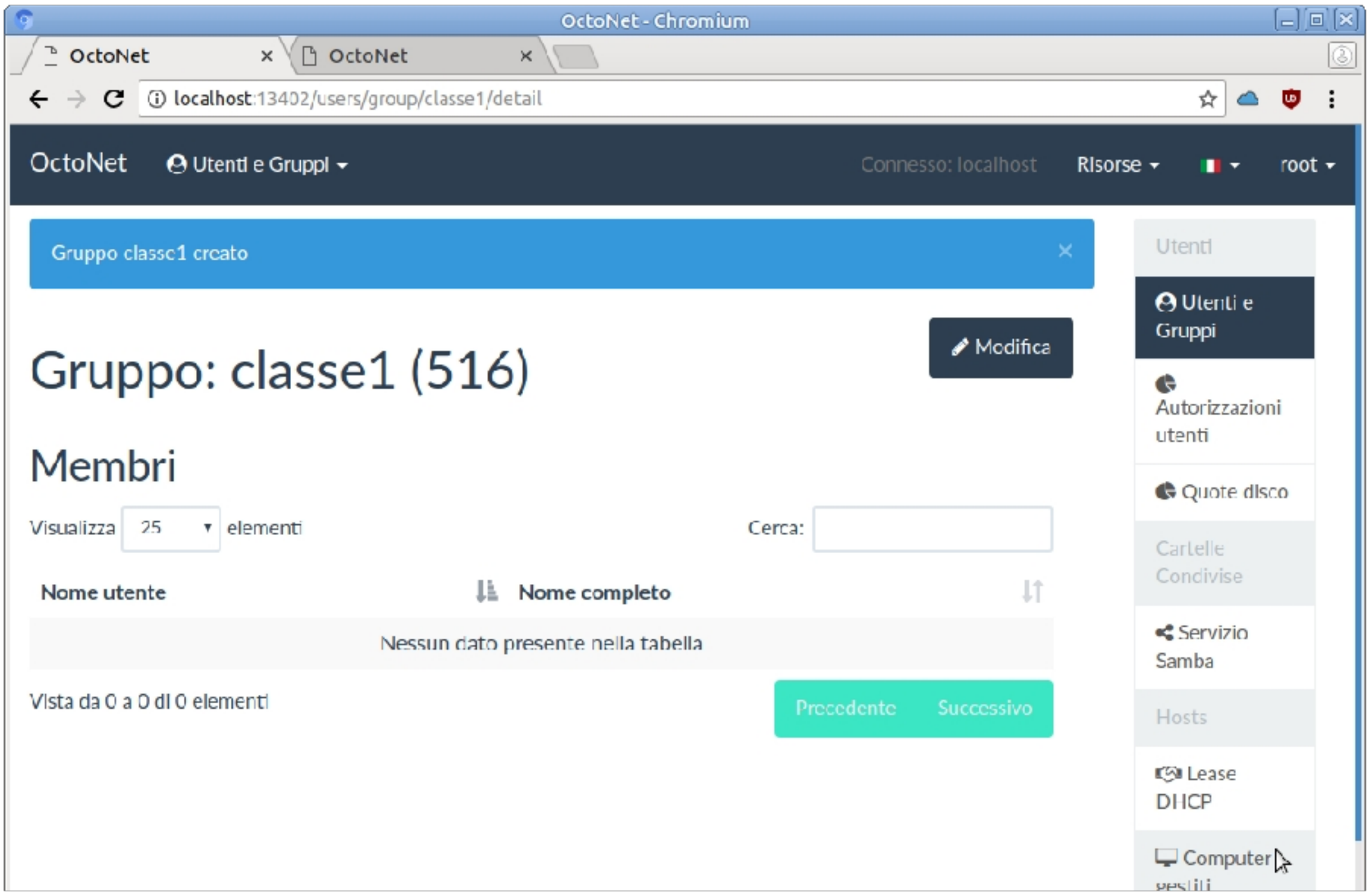
Keep in mind that before creating a user, if you want that user to be assigned to some specific group, the latter must exist. The list of groups *of* obtains from the menu *Users and Groups -> All Groups*, some of which are automatically defined (for Samba use) upon installation of *Fuss Server*, and are those shown on the following page:



From this page you can add a new group with the *Create New Group* button or by selecting the same feature from the *Users and Groups* menu, you will get the creation page:

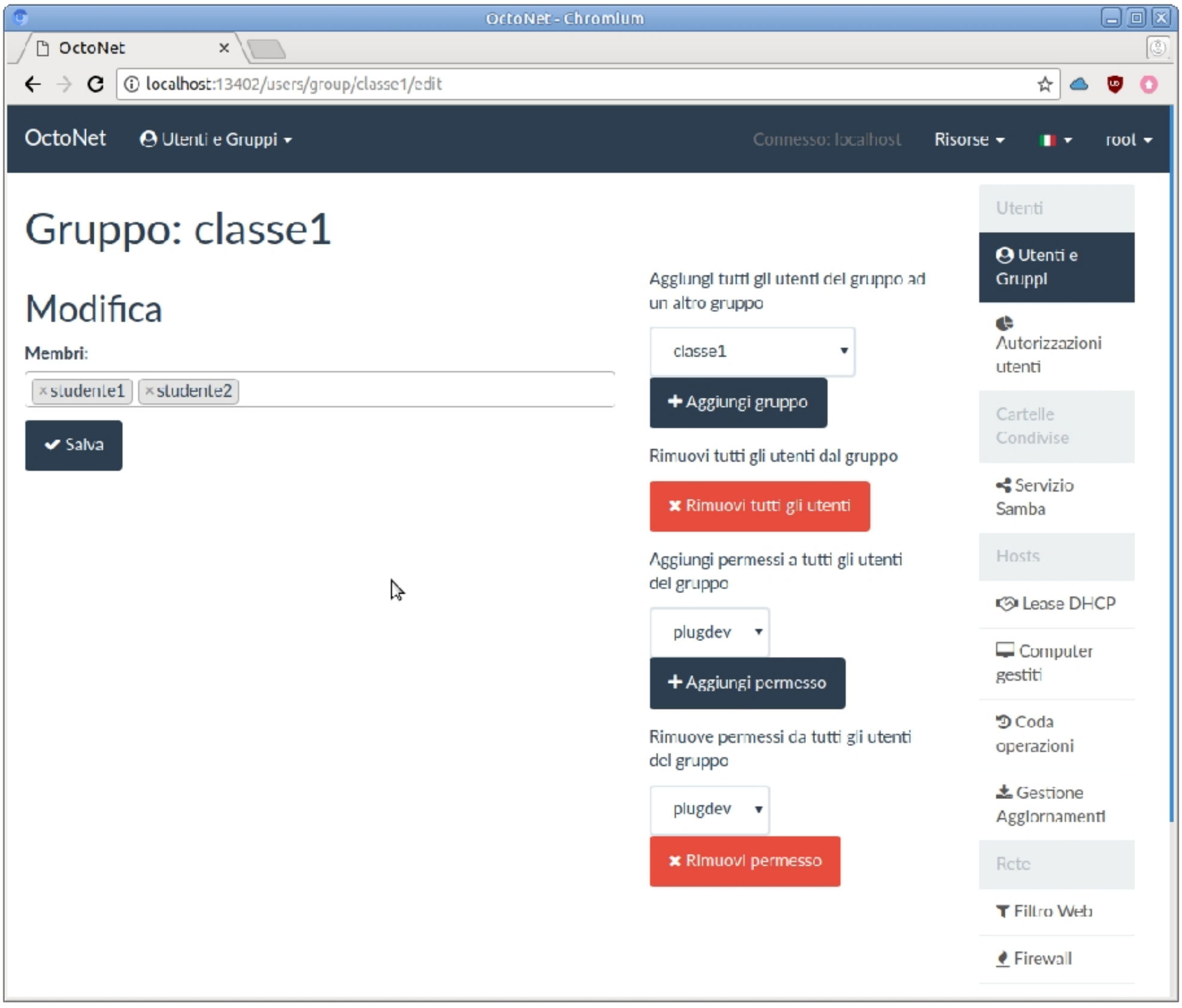


in which you must enter the name of the group (which must be given using only lowercase letters and numbers, no spaces or other punctuation characters). Once the group is created you will be taken back to its page, which lists its members (none at first):



It is appropriate to create a group for each class you want to define, and any other groups by user type (technical, secretary, faculty, etc.). But keep in mind that the teachers group (or any group whose name begins with `docent`) has a special role for managing password expiration according to privacy regulations, and is reserved for teachers' users.

Once you have created a group it can be used on the management or user creation pages, and users can be added or removed from it. Also, pressing on the *Edit* button in the upper right corner will take you to the group management page:



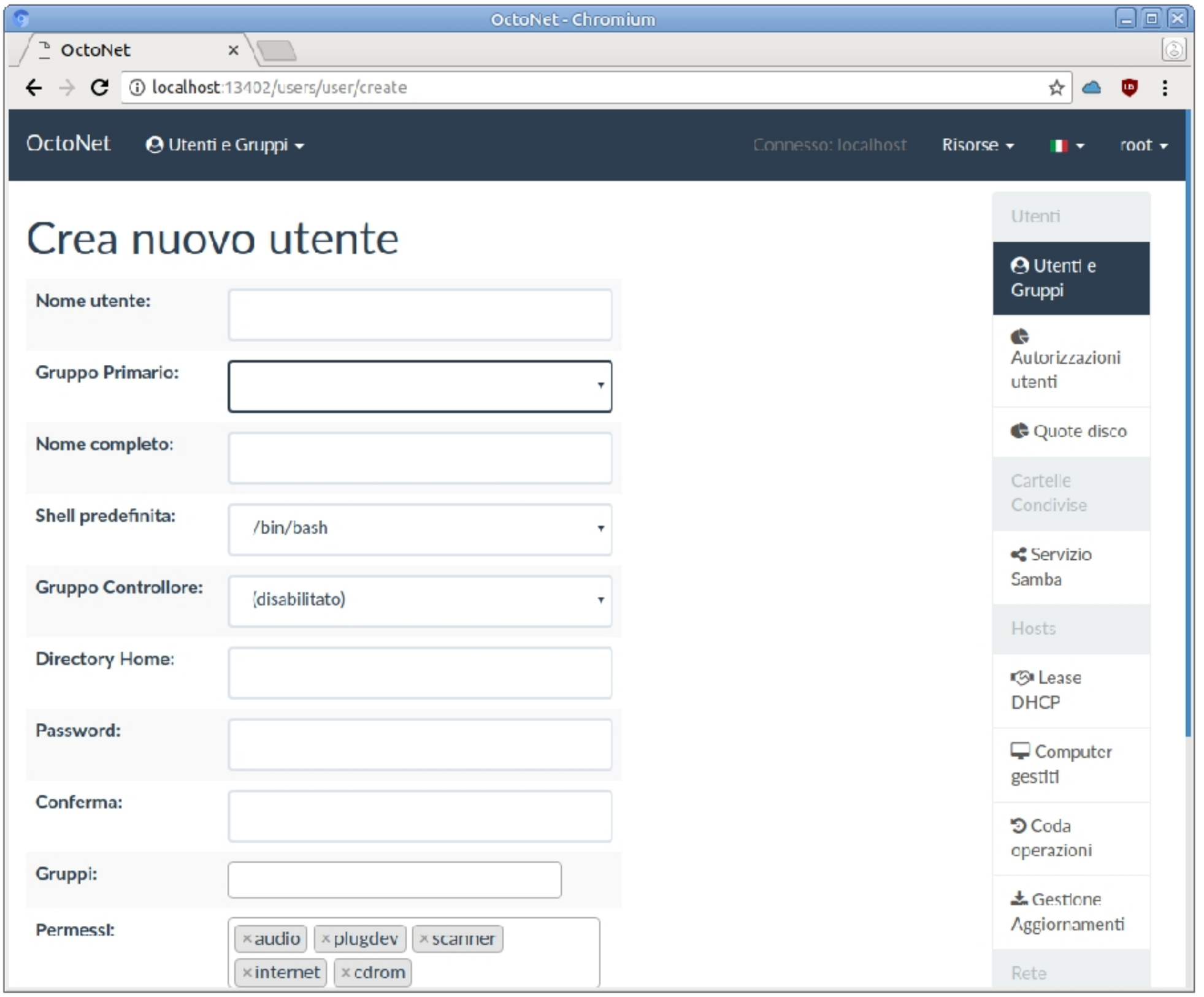
The members present are shown in the *Members* as buttons text box, and can be removed from the group by clicking on the cross in the button, clicking instead in the empty area will present a drop-down menu with available users with which new members can be added to the group. Once the changes are complete they should be saved with the *Save* button.

Further operations are possible with the buttons on the right, in which case the application is immediate and once the operation is done you are returned to the group page; the operations are:

- with *Add Group* you can add all users in the current group to another group, selected from the drop-down menu above;
- you can remove all users from the group at once with the *Remove All Users* button;
- you can bulk add Permissions to all users in the group with the *Add Permission* button, selecting which Permission from the drop-down menu above;
- similarly with the *Add Permission* button you will be able to remove a permission, again to be selected from the drop-down menu above, to all users in the group.

5.2.3 Single user creation and management

Once you have created the groups needed to create a user you need to select *Users and Groups -> Create User* from the *Users and Groups* management menu which takes you to the creation page shown below:



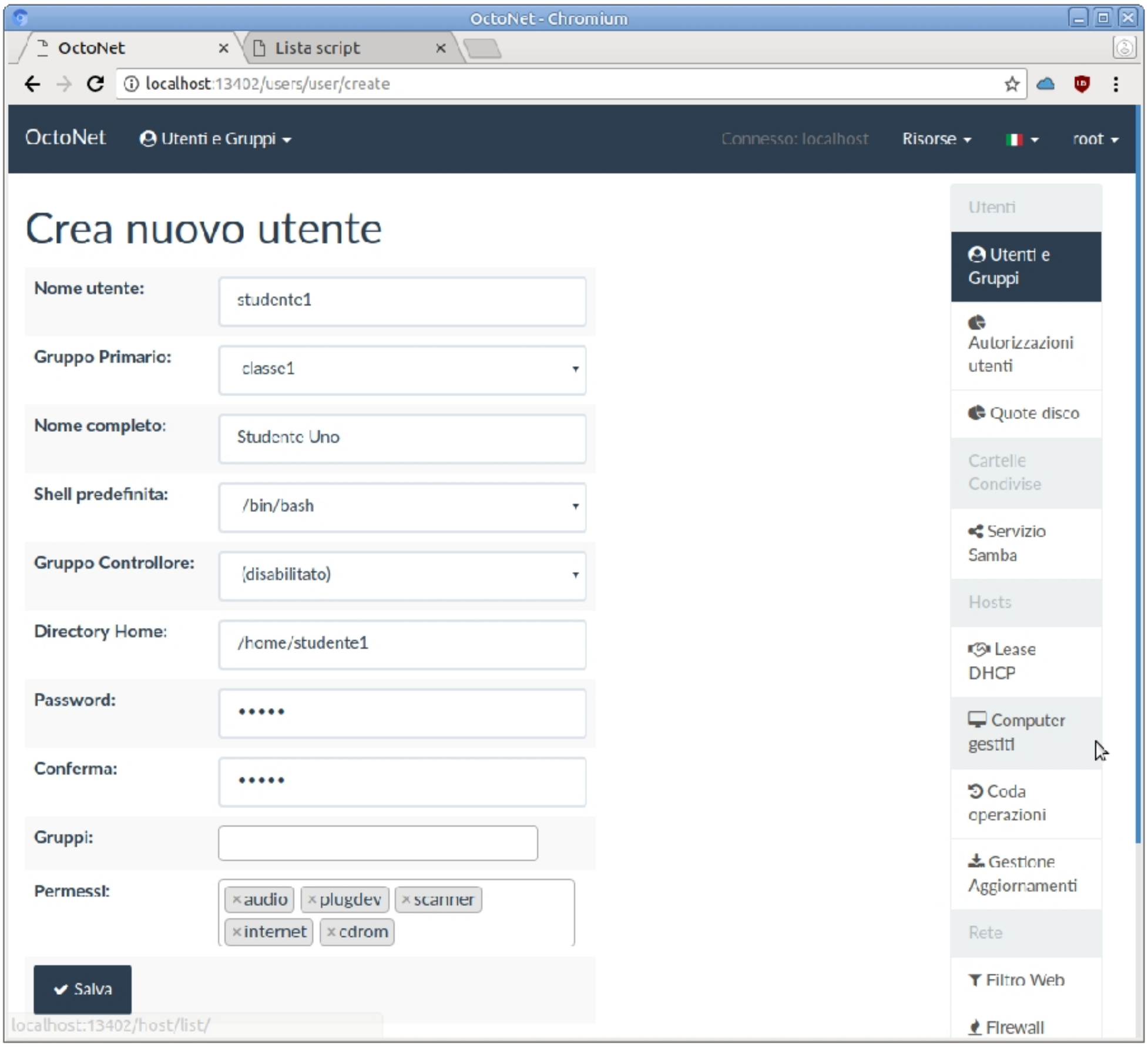
In this case it will be necessary to first specify a user name, again it is necessary to indicate the same using only lower case letters and numbers, without spaces or other punctuation characters, in writing it will automatically validate the *Home Directory* field with the default (which is always `/home/user name`). If the user is a student, it is appropriate to indicate as the *Primary Group* the one corresponding to his or her class, and to indicate its full name (capitals and spaces can be used here) in the field of the same name.

The fields *Default Shell*, *Controller Group*, and *Home Directory* can be left at the default; you can possibly change the latter if you have decided to subdivide student homes by class, using a path such as `/home/students/classroom/nameschoolhome`.

The password must be entered twice (same in the *Password* and *Confirmation* fields). Any additional groups you want the user to be a part of should be indicated in the *Groups* field (clicking inside shows those that match the entered text in a drop-down).

The *Permissions* field is used to control the permissions that will be assigned to the user so that the user can use the relevant features when logging onto a client. These correspond to as many local client groups in which the user will be automatically placed (keep in mind, however, that this is not immediate; the client needs to be turned on and synchronize with the server, so it can, at worst, take up to 5 minutes for this to happen).

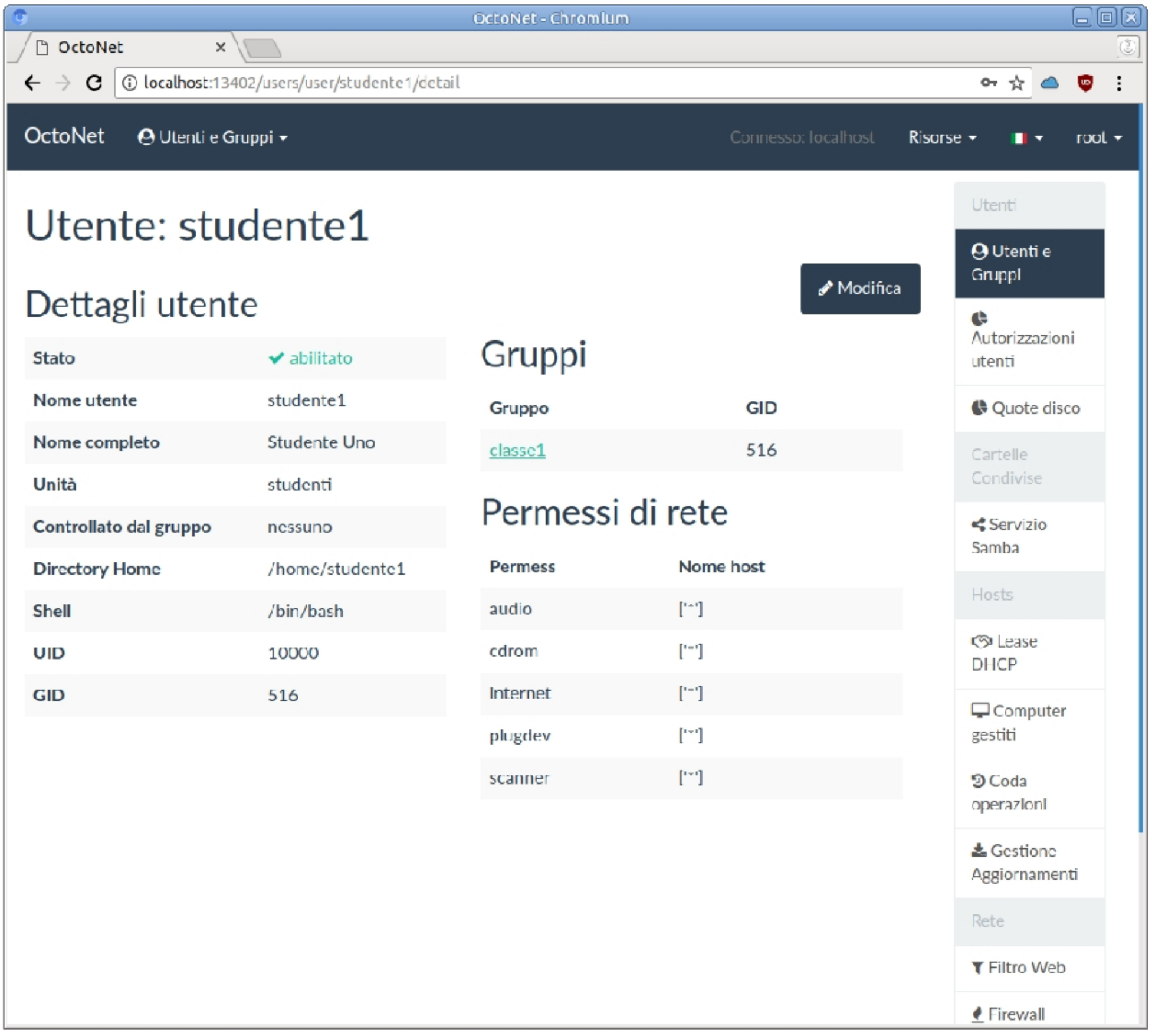
Also, for Internet browsing to be enabled, the `nscd` cache must be refreshed: to force an update, you can use *the Propagate network access permissions* item in the *Users and Groups* menu.



The default proposes permissions for access to the sound card, removable devices, scanner, Internet and CDROM, according to the list in the table.

Permit	Meaning
plugdev	Can use removable devices (USB sticks, etc.).
cdrom	Has access to CDs and DVDs
audio	Can use audio devices (sound card)
video	Can use video recording devices (ex. webcams)
internet	Can surf the web through the proxy
scanner	Can use a scanner
lpadmin	Can administer printers
bluetooth	Can communicate with bluetooth service through dbus
netdev	Can administer network interfaces via Network Manager

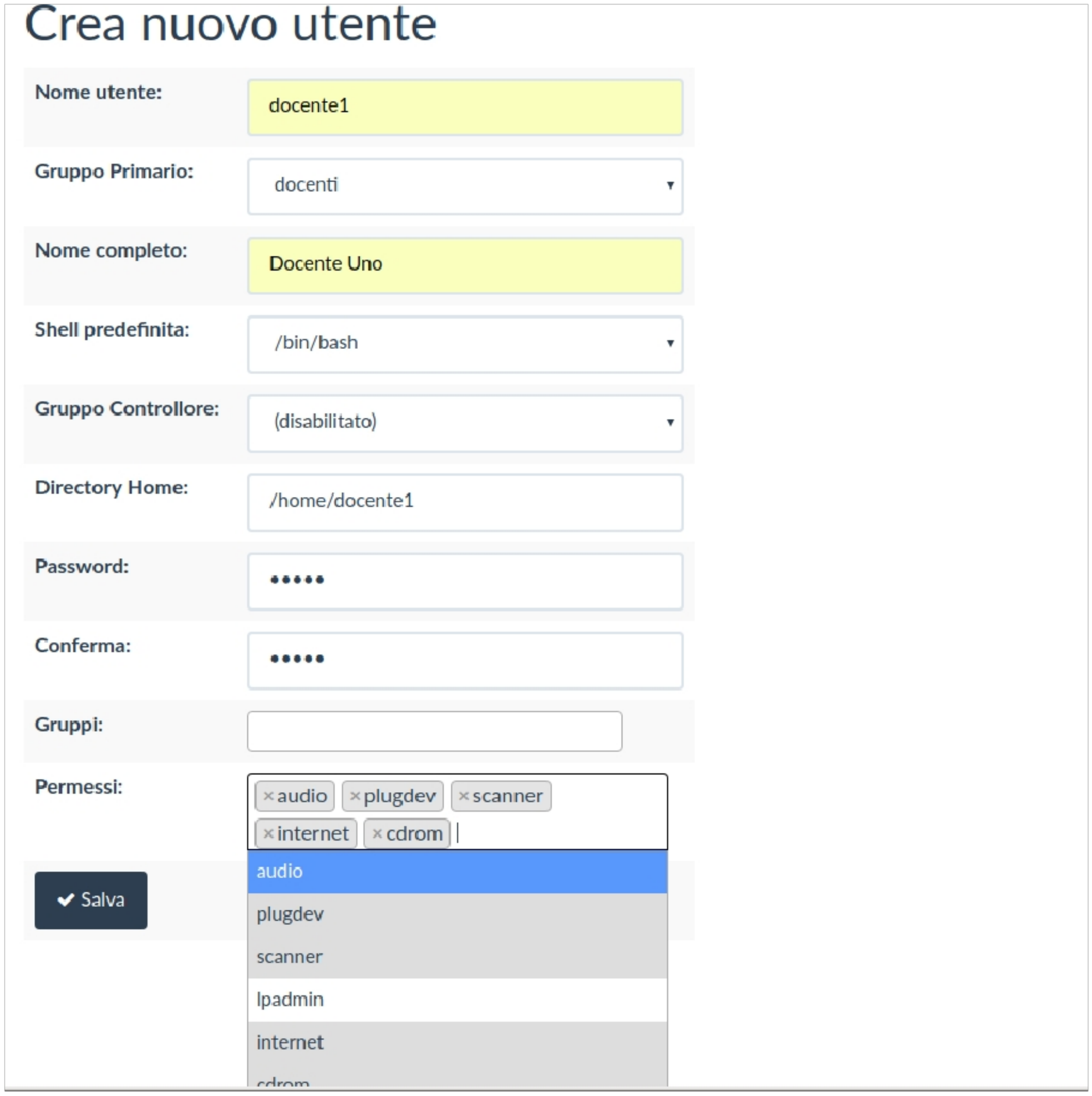
By clicking on the cross they can be removed, clicking in the field will show a drop-down menu showing the ones available, with those in gray, and more can be added. Once you press the *Save* button the user will be created and you will be taken to the relevant management page:



Note how the user, not having been classified as a teacher, carries the value *student* in the *Units* row. As mentioned, this parameter is handled automatically based on the user's main group, and it determines how password expiration is handled, which is not there for a student (who does not process personal data) while it is enforced for teachers according to the requirements of the privacy regulation.

In case you want to create a user for a teacher it will then be necessary to use as the main group (**note**, main group, in the *Primary Group* item and not in one of the auxiliary groups indicated in the *Groups* item) a group whose name begins with the string `docent` (it is thus possible to create more than one group for teachers, to differentiate any access rights, for example for the *Controller Group*).

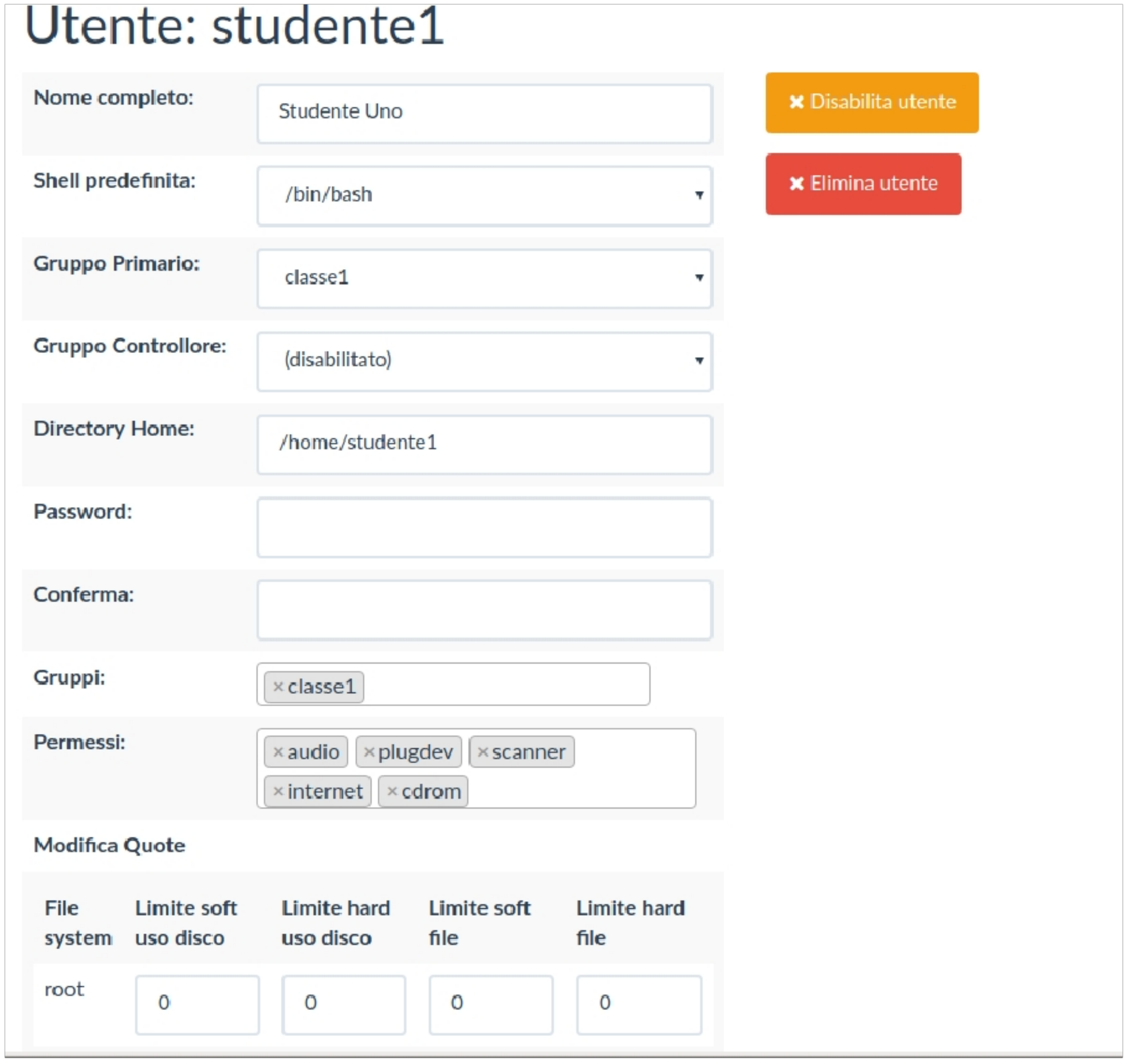
An example is on the following page, where in addition to using the `faculty` group, the user is also assigned the `lpadmin` privilege, which allows the user to perform printer management.



with the use of the `faculty` group as the main group, the new user will be classified in the *Unit* row
As a lecturer:

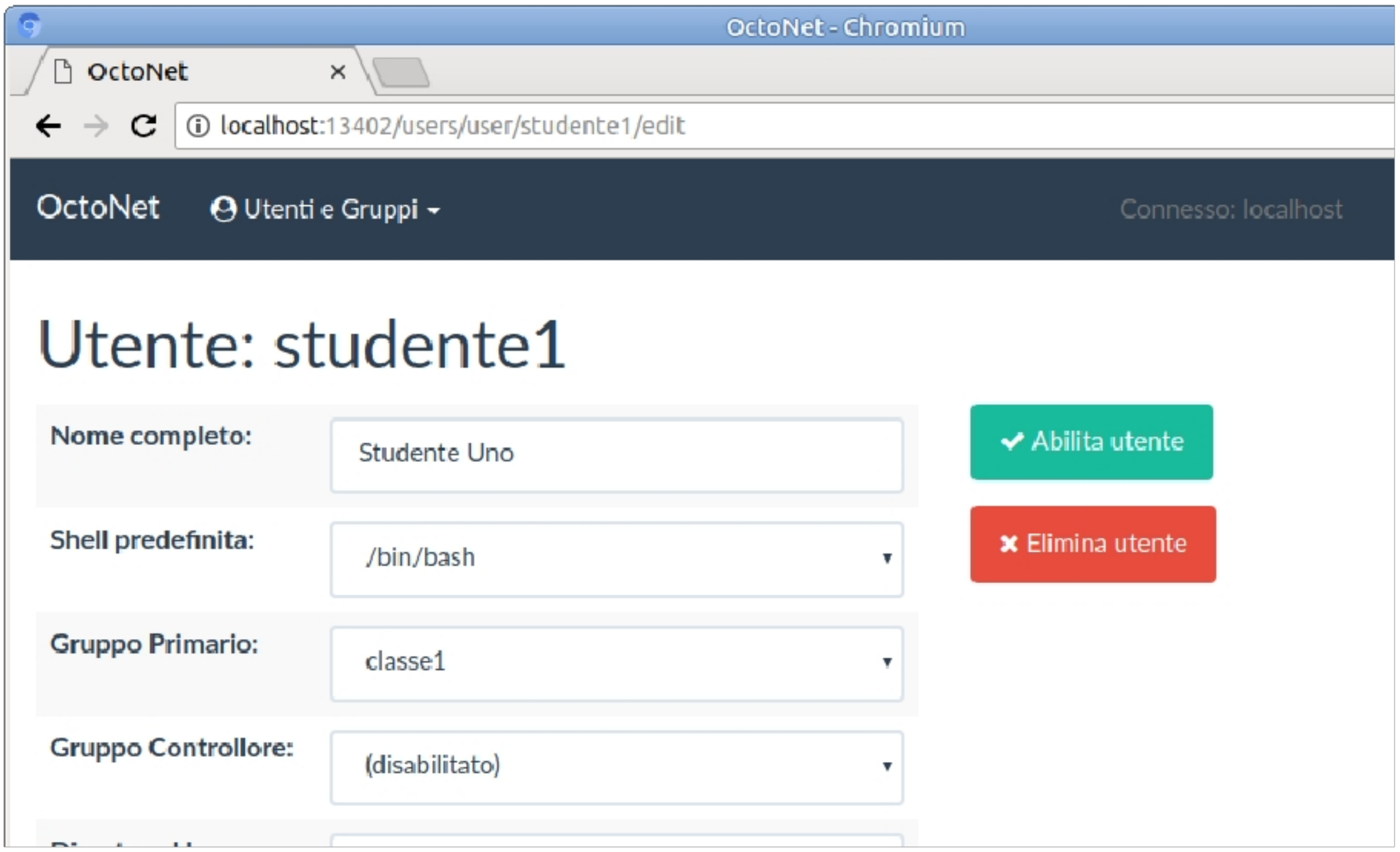


Once the user has been created, you can change its settings, disable it or delete it by clicking on the button *Modification* of its management page:



From this page, in addition to changing the properties entered during creation (all except the user name, which cannot be changed via *OctoNet*; if you made a mistake you have to delete it and create it from scratch), some additional operations are possible:

1. you can (when configured and enabled) enter the user's disk quotas (in the *Edit Quota* section)
2. you can delete the user with the *Delete User* button; the user will be deleted and in order not to lose any of its data, a `username.tar.gz` archive will be created with the contents of its home directory in the directory under which it was located
3. you can disable the user with the *Disable User* button, in which case the user's access will be disab- lished, the user will be marked as disabled in the list of users and on their page, but their account will remain active and can be rehabilitated
4. you can rehabilitate a previously disabled user with the *Enable User* button that appears instead of the *Disable User* button on the edit page when the user is disabled.



Warning: WARNING! In case the `Edit` button takes us to the error page, it is possible that **quotas** have not been configured correctly (see https://fuss-tech-guide.readthedocs.io/ en/latest/quick-install.html#configure-initial-for-quotes). Anyway, to investigate the cause of the octonet malfunction, you can use the commands:

```
systemctl status octonet.service
```

or:

```
journalctl -u octonet.service
```

5.2.4 Manual management of users and groups

The best way to manage users is to use the octofuss interface, which automates the entire procedure while minimizing the risk of errors, plus it is the only one that allows management of user permissions. These notes are useful in case you need to intervene directly through the `smbldap-tools` instead. It is assumed that they are invoked as root on the server.

It is important to note that for proper operation of the home on the fuss-server, it is necessary not only to manage an LDAP/Samba user, but also the related Kerberos principal, with the same password.

The creation of a user can be accomplished with the command:

```
smbldap-useradd -a -m username
```

which must be followed by setting a password with the command:

```
smbldap-passwd username
```

You then need to set up a Kerberos principal with the same password, via the @kadmin.local@ command:

```
kadmin.local << EOF
addprinc user@DOMINIO.LAN
```

(continues on next page)

(continued from previous page)

```
pwd
pwd
EOF
```

Keep in mind that with these commands the value of the user's `ou` attribute indicating whether the user is a student or a teacher is not set. It can be set manually using the command:

```
ldapvi '(uid=username)'
```

which opens an editor with the contents in LDIF format of the user's data; adding the line:

```
ou: students
```

to the attributes shown in the editor will classify the user as a student. To

change the user's password you can use the command seen above:

```
smbldap-passwd username
```

and then also update the Kerberos principal password with `kadmin.local`:

```
kadmin.local << EOF
cpw user@DOMINIO.LAN
newpw
newpw
EOF
```

The command can be used to create a user group:

```
smbldap-groupadd -a nomegroup
```

To add a user to a group you can use the command:

```
smbldap-groupmod -m user-name group-name
```

While to remove it:

```
smbldap-groupmod -x user-name group-name
```

To temporarily disable a user you can use the command:

```
smbldap-usermod -I username
```

And to rehabilitate it:

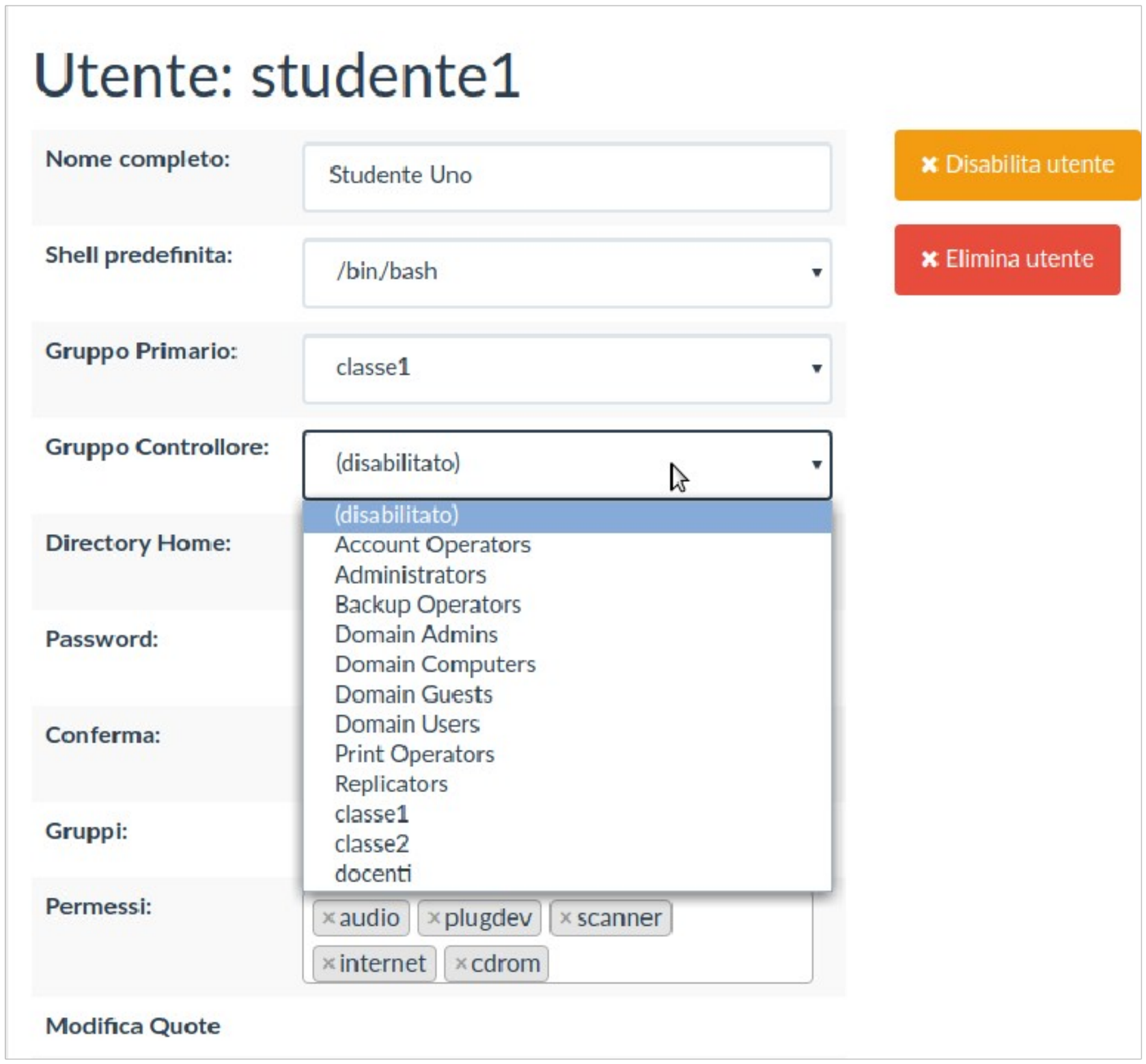
```
smbldap-usermod -J username
```

5.2.5 The controller group

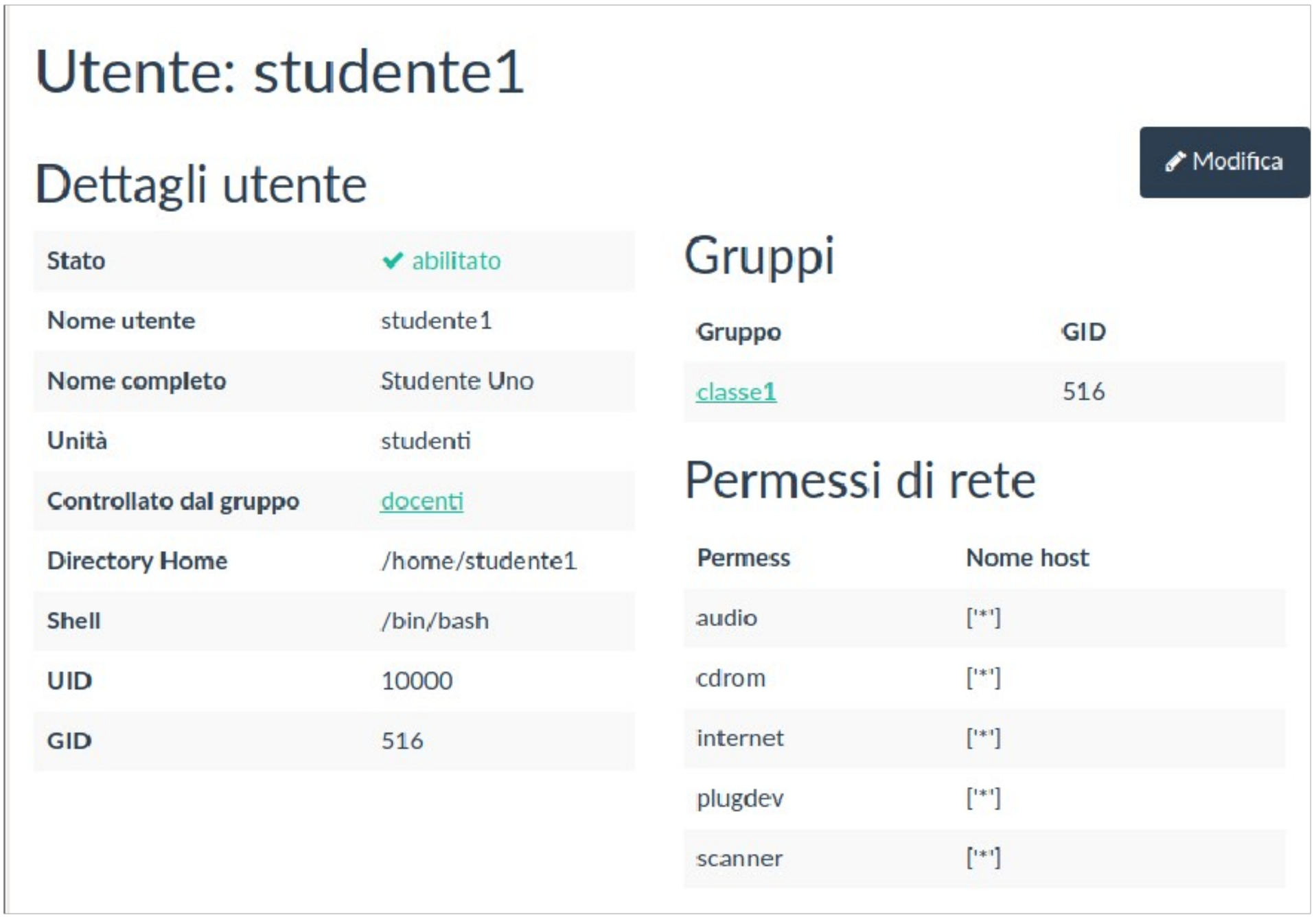
In the creation of a user his home will be created with permissions `0700` (i.e., accessible only to him) by assigning the user ownership of it, while for the owner group the preset `Domain Users` group will be used, i.e., you will have in the case of the previous example:

```
root@fussserver:~# ls -ld /home/student1
drwx------ 2 student1 Domain Users 4096 Jul 23 18:22 /home/student1
```

it is possible, however, to provide access to the contents of the home to users who are part of a group (called the *Controller Group* for this) to be specified in the field of the same name on the user's management page (e.g., the `faculty` group) by clicking on which you get a drop-down menu on the available groups (on which a search is automatically performed on what you type in the field) from which to choose:



and once a controller group is set up it will appear on the user page:



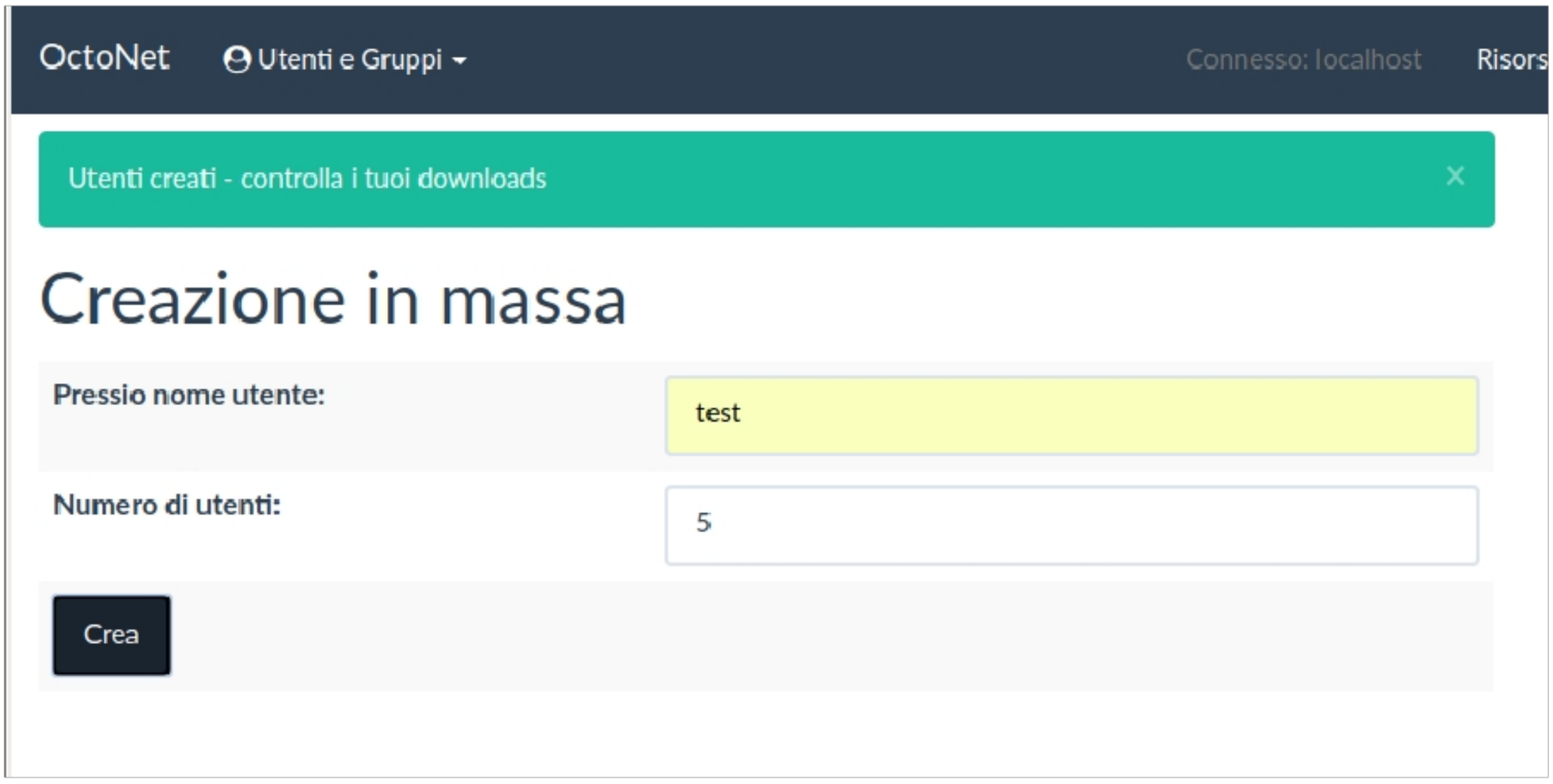
And the permissions of his home will be changed to `2770`:

```
root@fussserver:~# ls -ld /home/student1
drwxrws--- 2 student1 faculty 4096 Jul 23 18:22 /home/student1
```

in this way the `faculty` group will have read and write access to the contents, and new files and directories will be assigned to the group as the owner group.

5.2.6 Mass user creation

The feature, mainly provided for testing purposes and to create temporary user blocks (e.g., for access to be provided to outsiders in a test exam) is accessible from the *Mass Creation* item of the *Users and Groups* menu and requires entering a prefix and a number of users to be created:



users are created and a file (`mass-created-users-AYYY-MM-DD.csv`) is automatically made to download, in which a list of them and their respective passwords are automatically assigned.

There is no bulk delete functionality, but this can be accomplished relatively quickly using `octofussctl` from the command line with:

```
export
OCTOFUSS_PASSWORD=password echo
ls users/users/test* \
  | octofussctl http://localhost:13400/conf -u root \
  | tail -n +2 | tr -d " />" \
  | sed -r 's|([a-z0-9]+)|delete users/users/\1|' \
  | octofussctl http://localhost:13400/conf -u root
```

which unlike manual deletion with other user management tools, performs the deletion as if you had done it from OctoNet, creating archives with user files.

5.2.7 Create users from CSV file

A second feature for mass creation of user lists is import from CSV files, which allows a list to be prepared in a `.csv` file.

File format

The CSV format has many variants, of which a limited subset is supported, hence some precautions in creating the CSV file to be used for import, which must have these characteristics:

1. **Encoding**: the encoding of the file must be ASCII or UTF-8 without BOM. The BOM (Byte Order Mark) we have seen create problems. You can verify that the encoding is correct by running the command:

   ```
   $ file nomedelfile.csv
   ```

   And if the result is:

   ```
   nomedelfile.csv: UTF-8 Unicode (with BOM) text, with CRLF line
   terminators
   ```

   Will need to convert it this way:

```
$ uconv nomedelfile.csv -t ASCII > newfile.csv
```

and you can then verify that `newfile.csv` will have the correct encoding:

```
newfile.csv: ASCII text, with CRLF line terminators
```

2. **Text fields**: fields should be in alphanumeric format avoiding control characters such as comma or superscript, this is necessary for user and group names, but also applies to names and passwords, so punctuation and punctuation characters should be limited.
3. **Consistency of number of columns**: In the file all rows should have the same number of fields. For example, here we see the first row contains 4 fields, and the second contains 5:

```
Mario,Rossi,mariorossi,mariorossipassword
Lucia,Bianchi,luciabianchi,luciabianchipassword,additive field
```

and this will also not do; also keep in mind that an empty line, even if put at the end of the file, is considered to have 0 fields (the carriage return on the last line does not count, but there must not be any more) so a file that contains one will not do for this reason).

4. **File format**: The file should *not* have the first header line, but all lines should be related to users. For example, a file that starts like this:

```
Name,Surname,Username,Password
Mario,Rossi,mariorossi,mariorossipassword
Lucia,Bianchi,luciabianchi,luciabianchipassword
```

is no good, and you will need to delete the first line so that the file starts directly with the user-related lines. In this case, the requirement is not stringent, since the import interface allows you to exclude a possible header row.

Since if the file to be imported is very large examining the correctness (particularly for the third requirement) is not trivial, from the menu *Users and Groups -> Verify CSV File* a preventive check can be made:



Where you are prompted to choose the file to check (the desktop file selector will open) and the row where you entered the username (it will be checked for duplicates), if for example we start with a with an empty row file such as:

```
user,three,user3,foo,class2
teacher,two,teacher2,foo,teachers

lecturer,three,lecturer3,foo,lecturers
```

it will be necessary to denote the column with the username with the number 3, but containing this an empty row we will get:



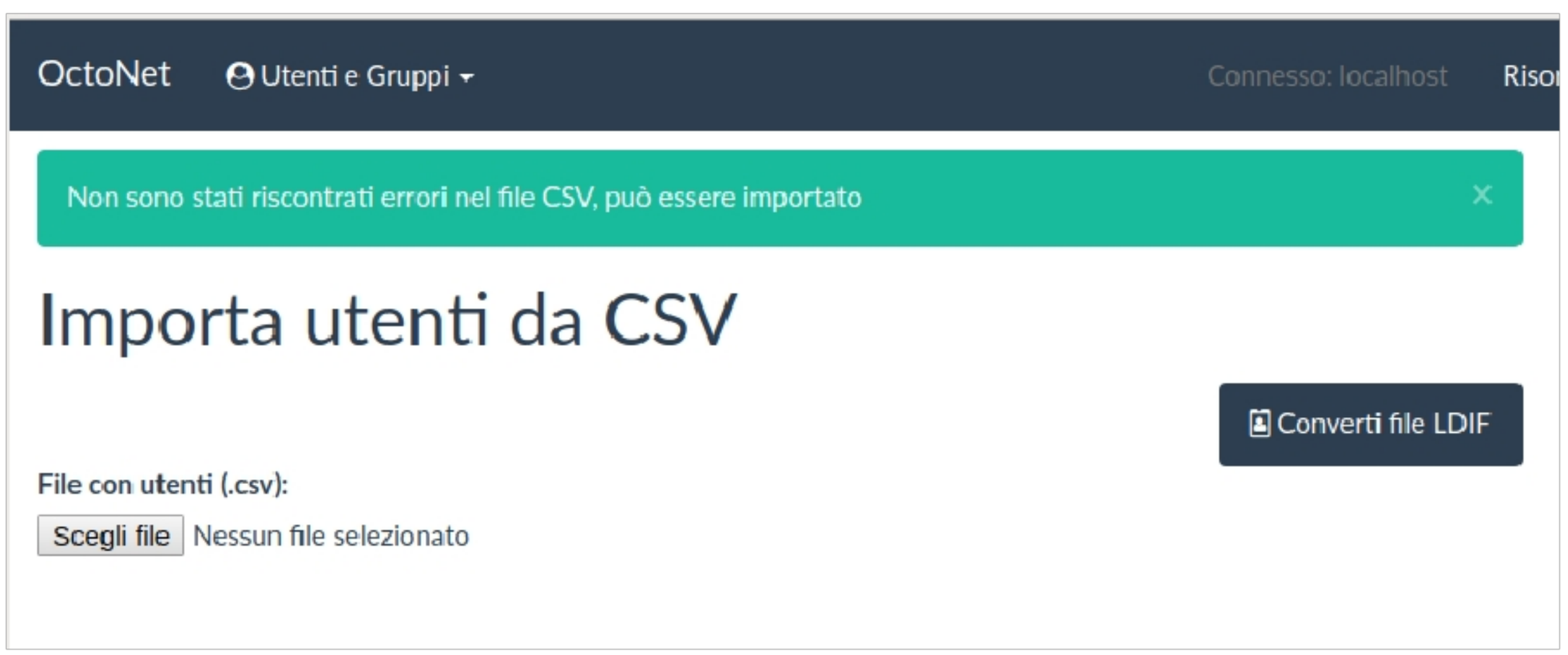
Instead by having a file with a username listed twice as:

```
user,three,user3,foo,class2
lecturer,two,lecturer2,foo,lecturers
lecturer,three,lecturer3,foo,lecturers
user,four,user4,foo,class1
student,three,student3,foo,class1
student,four,student4,foo,class1
student,five,student5,foo,class1
student,five,student5,foo,class1
```

we will get:



while if the file is correct (putting `student6` in the last line) we will get:



being automatically redirected to the CSV file import page.

This control is important because the import enters one user at a time and stops if there is an error, after which it is not immediate to pick up where you left off.

Prerequisites

The check on *Users and Groups -> CSV File Verification* only performs a basic consistency check of the file contents; for the final import to be successful, a number of additional requirements are needed:

- Any primary groups or controller groups indicated in the file must already be present in the system (bi-sogically create them first always through *OctoNet*). If any are missing, the system will give a message of

error without importing anything, to avoid partial imports. This does not apply to secondary groups, which are created in the import instead.

- No users listed in the CSV file should exist on the system.
- No home directory of those that should be created during the import should be present. Remember that for

professors, the primary group to add them to is `lecturers`, not `teachers` or `professors` or other. So this will have to be the primary group indicated, for professors, in the CSV file. The name is critical because it is on the basis of the name that the system understands that you are dealing with a teacher and not a student.

The file can contain the following fields (the field name refers to the name used in the import interface):

Field name	Format
Name	Name (one word)
Last name	Last name (one word)
Full name	First and Last Name
Password	password (avoid commas and CSV characters)
Username	username (lowercase only, any numbers in the tail)
Primary group	name of a group (must exist)
Controller group	name of a group (must exist)
Secondary groups	names of groups separated by spaces
Home Prefix	pathname of the directory where the home

Import procedure

For importing users from a CSV file you should use the page *Users and Groups -> Import from CSV*, which allows you to select a file from your machine with the *Choose File* button, you will get a table display like the following:



Now you will need to select the columns you wish to import by simply dragging the header cells to the desired column (from the other columns or from the list of unassigned columns at the bottom of the table); if a column you do not want or should not import, drag its header out of the table and the header will remain unchecked.

The interface also allows deletion of the first few rows of the imported file (starting at the beginning of the file only). This can be useful if the CSV has a header line (such as what can be obtained from converting an `.ldif` file). This is done by clicking on the corresponding line that will be crossed out; an example is shown in the following image:



clicking on the next row can be excluded as well, clicking again will remove the exclusion (again it only works on the last of the excluded rows, the exclusion functionality only applies to the beginning of the file).

The *Full Name* field cannot be imported if it is used to coincide with *First* Name or *Last Name*, if you use these two fields it is automatically created by merging them.

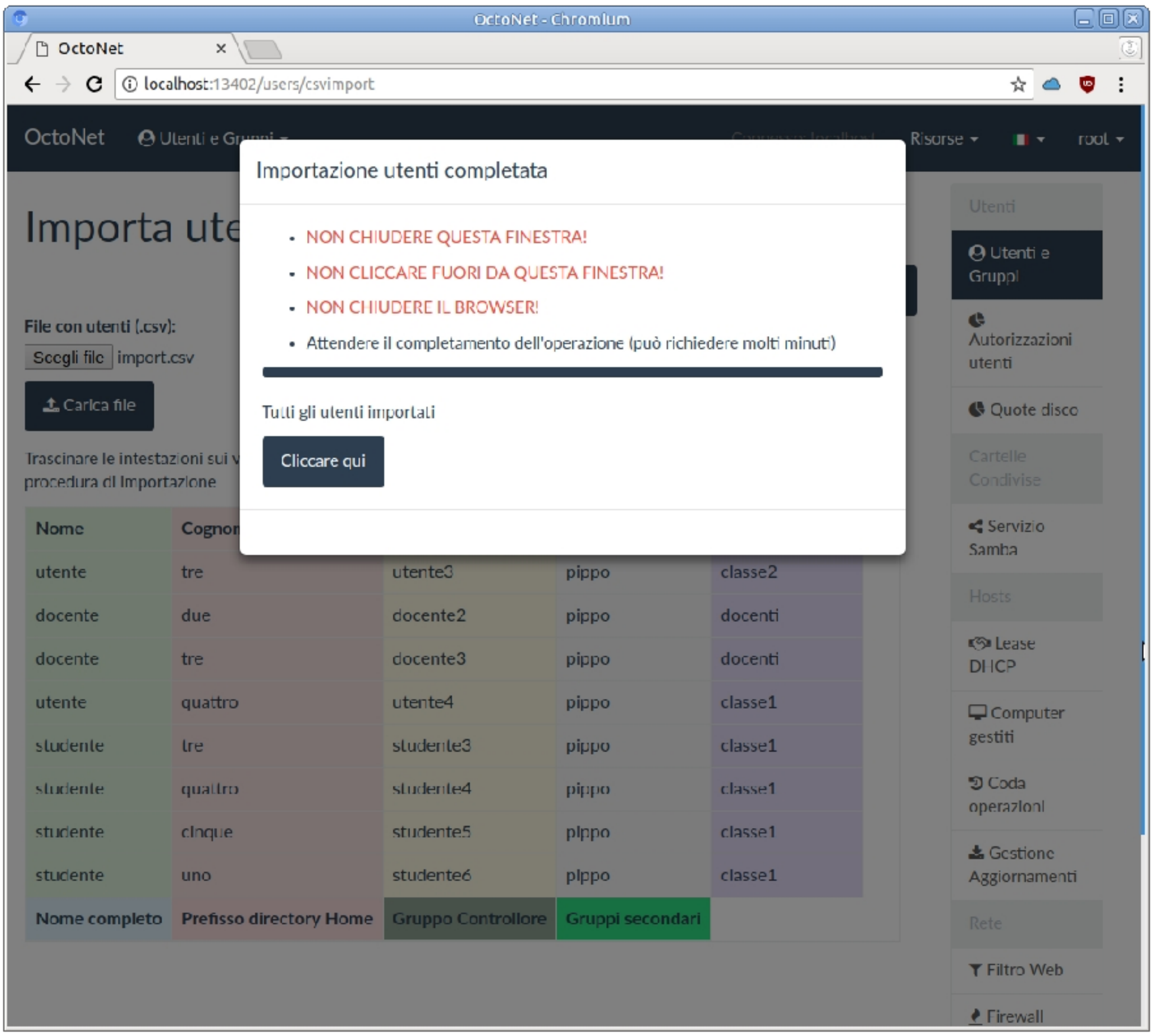
It is always mandatory to select the *User Name* column, if you do not do so the import reports an error and does not go forward.

If the password column is not set, users will be created without a password (and will not be able to log in until one is set for them). Once finished you should have a situation like this:



Once the columns are set up you can press *Upload File* and if everything is initially correct you should see a popup telling you not to close the window and to wait for the process to finish. This could take several minutes, or if you are dealing with thousands of users, even hours (this is an inherent limitation of LDAP).

If everything has been imported correctly, a button will appear at the end to redirect to the user list, where you can verify that the import was successful.



Importing from an LDIF file

If you have the user list in LDIF format (which can be obtained from a backup of them, available under `/var/backups/slapd` if you have installed and configured `fuss-backup`) you can perform a conversion of it using the *Convert LDIF file* button in the upper right corner. You can still get an LDIF file from the current instance with the `slapcat` command, with:

```
slapcat -v -l filename.ldif
```

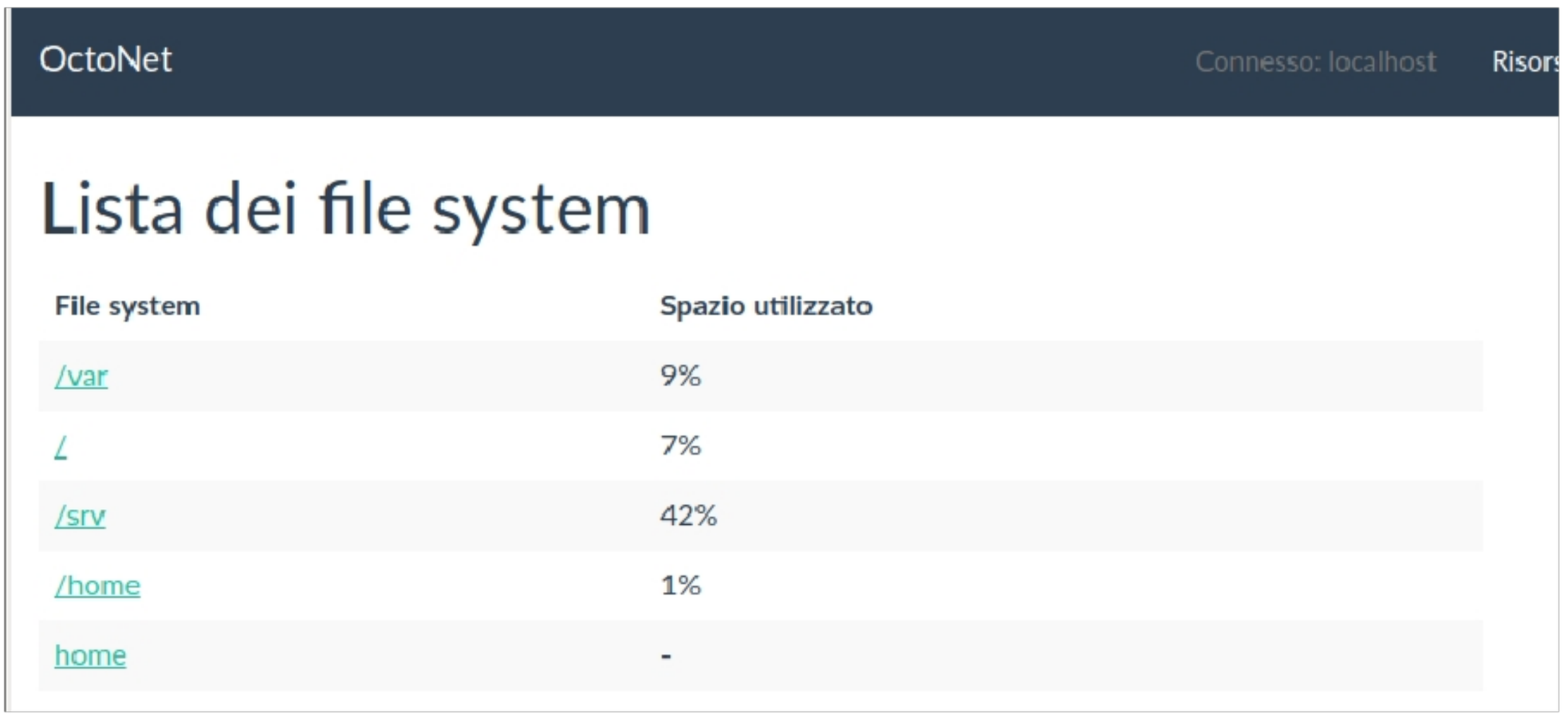


In this case you will have to choose a `.ldif` file with the *Choose File* button and then have it generate the CSV by pressing the *Generate CSV File* button, this will be generated and made to download to the browser, and you can go to the import page by clicking on the new *Import Generated File* button.

Keep in mind that the file thus generated will contain random passwords created by OctoNet, and has a header line that must be removed before import.

5.2.8 Disk quota management

Disk quota management can be done for the individual user from his or her management page, or by directly using the management interface that appears in the menu under *Disk Quota* on the right-hand column of OctoNet. Clicking on it will take you to a page listing the available filesystems:

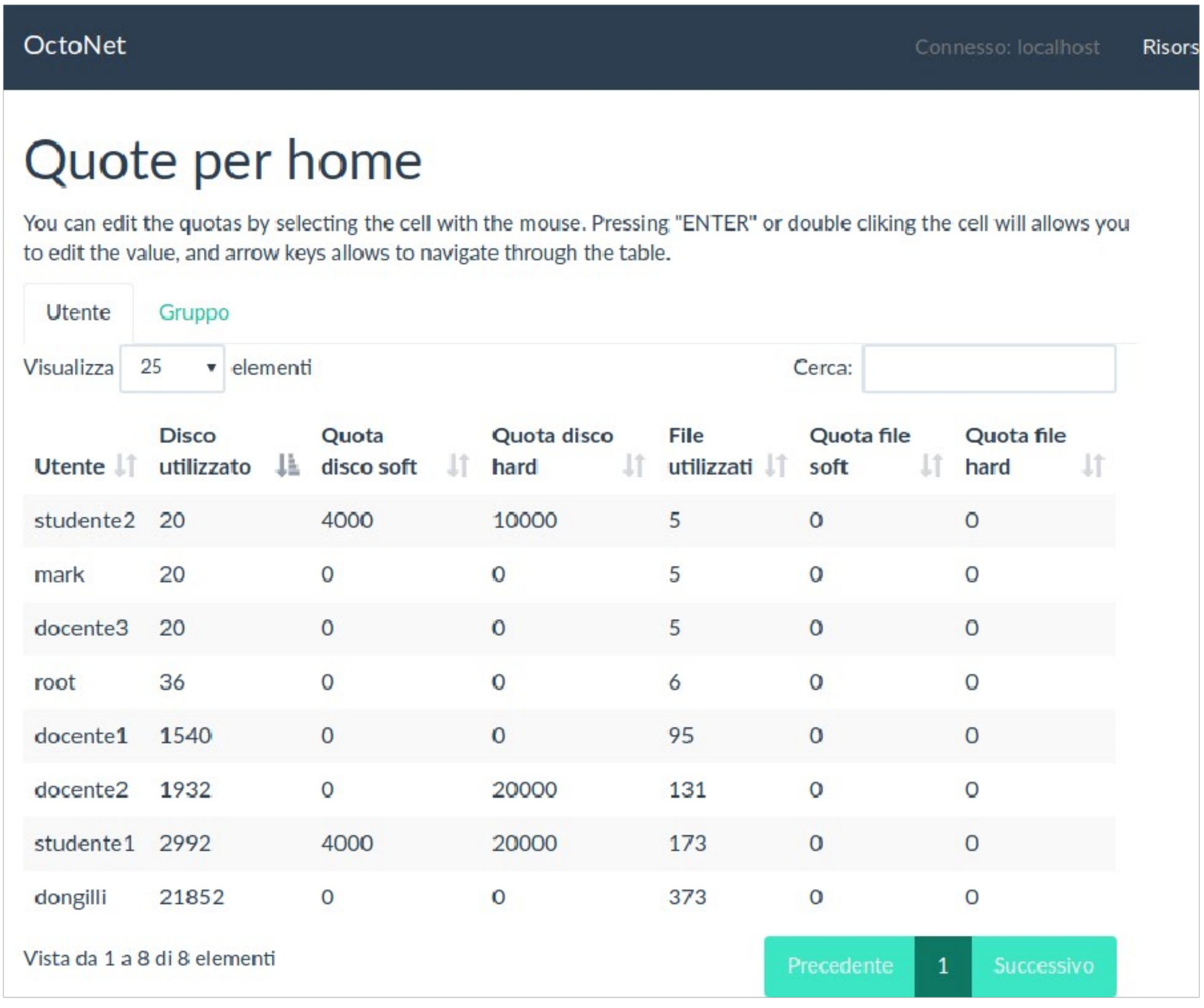


Keep in mind that the functionality is present only if disk quotas are active and configured. In ordinary *Fuss Server* installation this is done for the `/home` directory only if it is mounted on a separate filesystem.

In fact, disk quotas are applicable only at the filesystem level and not for individual directories. This also means, if data is distributed over several filesystems, that they cannot be applied in "global" form for a generic total but can be set only for each filesystem completely independently.

The page first lists the available filesystems indicating their respective *mount points* and disk space occupancy, and repeats at the bottom those for which disk quotas are enabled. *Fuss Server*'s choice is to enable them **only** for home, since it is only there that they make sense, applying to user data. Keep in mind that if you installed *Fuss Server* using only the root filesystem, they will not be active.

Although you can click on all filesystems you will get a list of quotas only for those on which these are enabled, in the previous case `home, so you` will get:



There are two types of quotas available, user quotas (which apply to the individual user) and group quotas (applied to files in a group), and they have two limits, *soft* and *hard*. The former can be exceeded for a limited period of time (the *grace time*, which by default is worth one week) after which it will be applied; the latter is applied immediately. User and group quotas are independent.

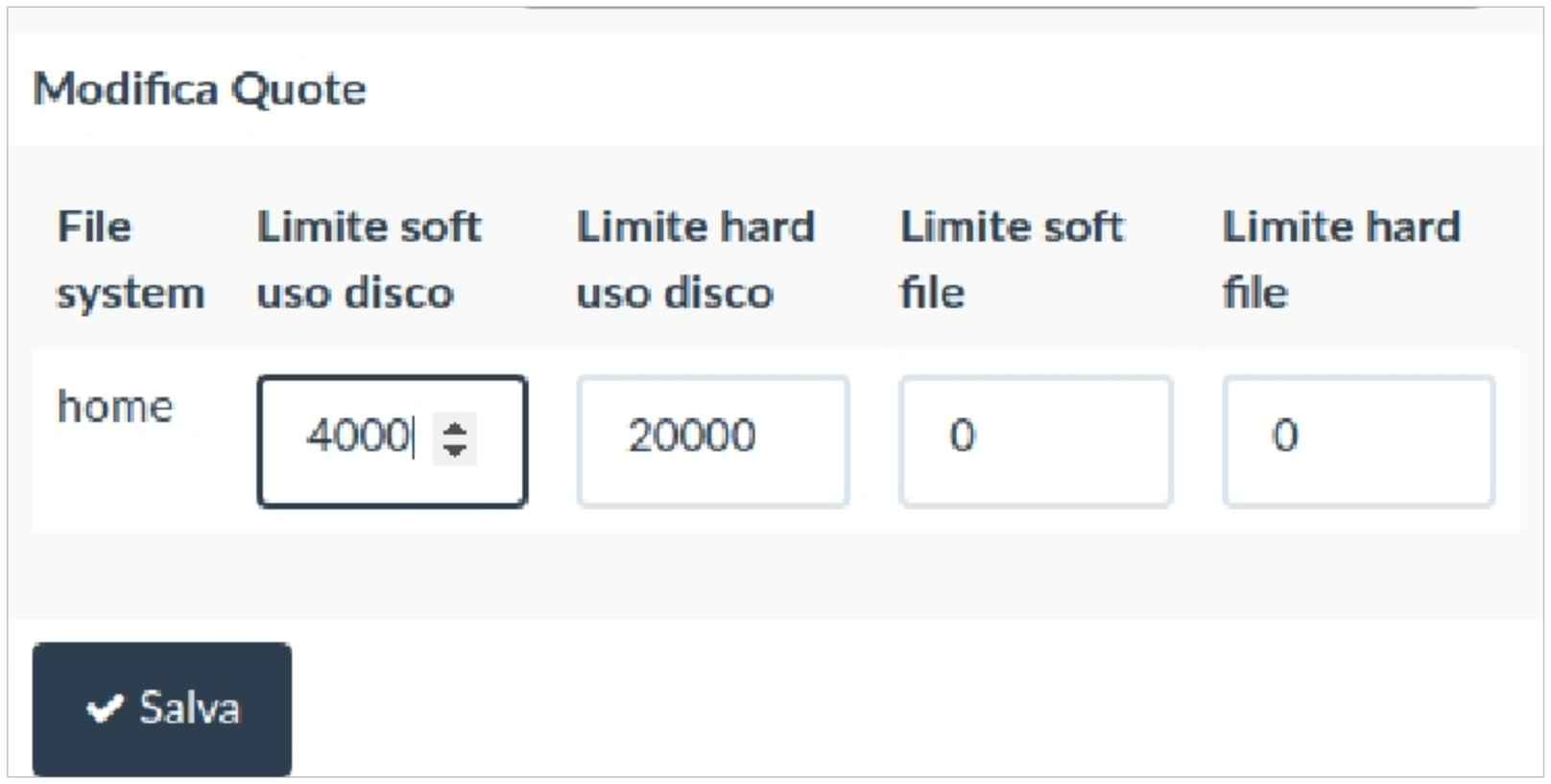
In addition, quotas are divided by disk space (*Disk Quota*) and by number of files (*File Quota*), and these are also independent of each other, i.e., you can exceed the quota either because you have run out of disk space, or because you have run out of files (so you will not be able to create new files, but you will be able to enlarge existing ones).

The page presents user quotas by default, you can switch to group quotas by clicking on the corresponding tab. A fixed number of users or groups selectable with the *View* drop-down menu are displayed, and you can search for a specific user/group with *Search*.

To change one of the values of the quotas double-click on it, and an immis- sion window will appear, you will have to specify a size in kilobytes for *disk quotas* and a number for *file quotas* and then save it; keep in mind that you should always indicate a lower value for *soft* quotas than for *hard ones*.



As mentioned, quotas can also be set on the individual user's management page in the final section of the user's edit page:

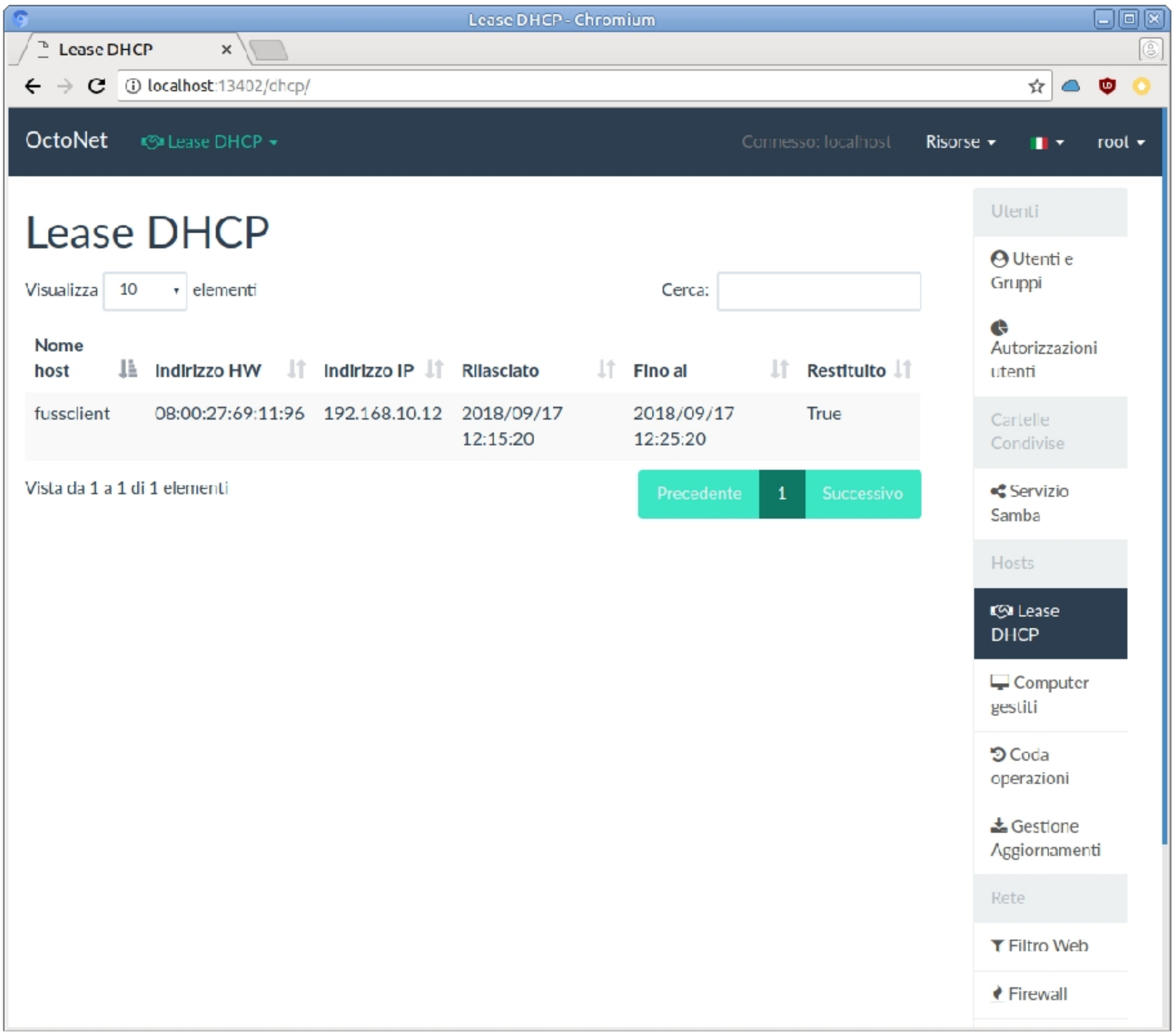


5.3 Management hosts

The *Fuss Server* can centrally manage clients that are part of a school network, using the features in the *Hosts* section of the menu on the right-hand column.

5.3.1 DHCP Management

The DHCP management pages can be accessed from the *DHCP Leases* entry, which automatically takes you to the page that lists the current status of the *leases* (i.e., MAC Address/IP Address assignments) on the server, and brings up the *DHCP Leases* menu in the top bar on the left.

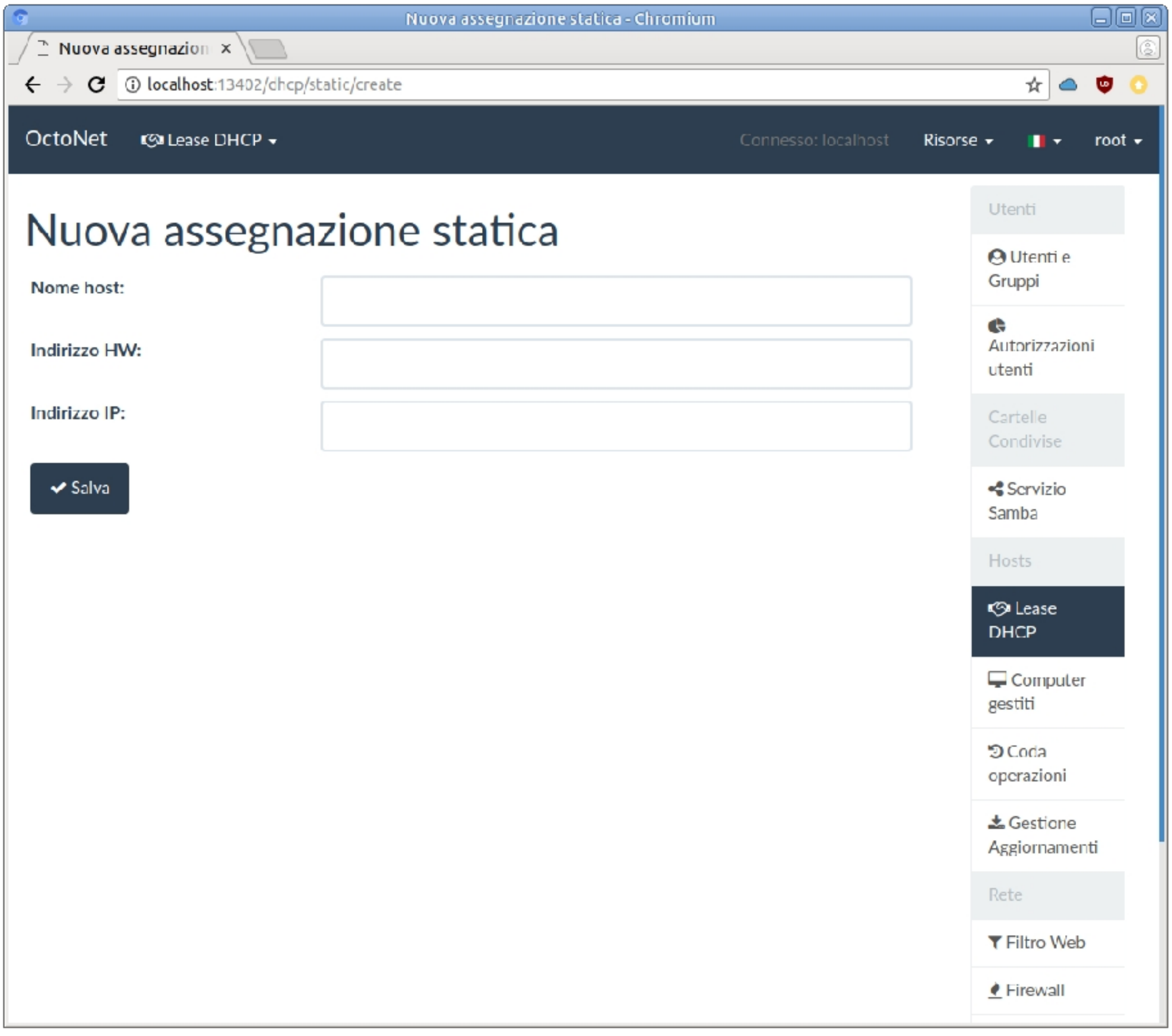


to the same page can be returned from any of the others in the section using the *DHCP Leases served* link from the *DHCP Leases* menu.

Recall that during installation of *Fuss Server* one of the requests made by `fuss-server create` is for the indication of the range of IP addresses to be dynamically assigned, which is stored in the `fuss-server.yaml` configuration file, in the `dhcp_range` variable; it can therefore be obtained with the command:

```
grep dhcp_range /etc/fuss-server/fuss-server.yaml
```

The page shown is informational only and tells us which dynamic assignments have been made; however, it is also possible to set up static assignments (so-called "reservations") using the *Create Static Assignment* item from the menu, which takes you to the relevant entry page:

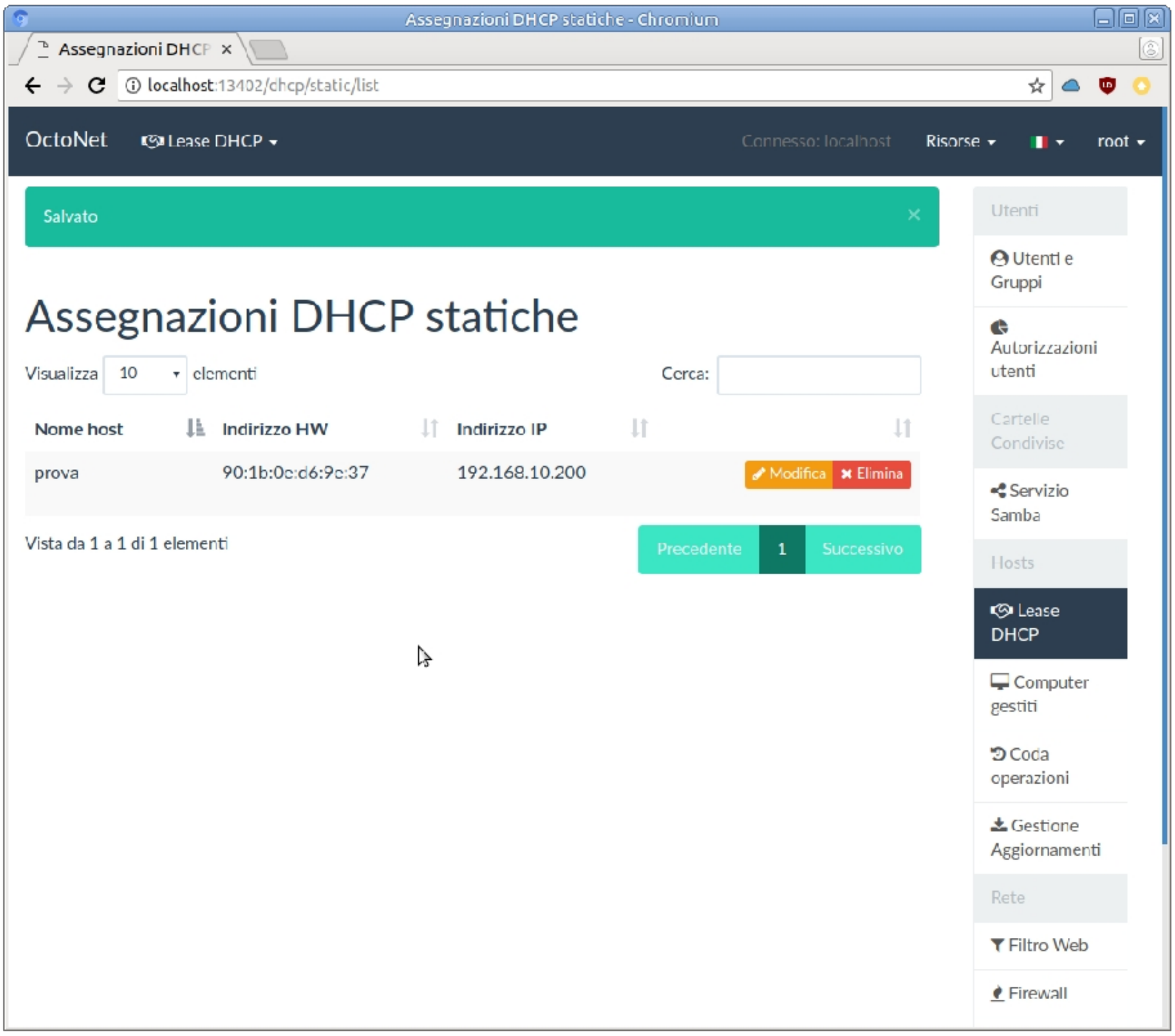


and in this way the addresses assigned to individual machines can be controlled through DHCP (this can be useful, for example, for assigning fixed IPs to network equipment such as printers so that their access can be centrally managed). It is generally not appropriate to use this assignment for clients, which are managed directly by the server, but only for external machines and equipment.

The page prompts you to enter a name that identifies the device, the MAC address of its network card, and the IP address you want assigned to it. It is appropriate that the latter be outside the dynamic IP range identified earlier. The setting will be saved in the file `/etc/dhcp/dhcp-reservations`.

Keep in mind that if the apparatus is set up to receive the address in DHCP, it will be dynamically assigned once you log on, and even if you then make a static assignment, it will not be made until the previous lease expires. Therefore, to make the static assignment effective, it is usually necessary to reboot the apparatus (or force a new request for an IP address, if there is a feature to do so).

Having made the assignment you will be taken to the page listing the assignments made, which can also be accessed directly from the *DHCP Leases* menu with the *DHCP Static Assignment* item:

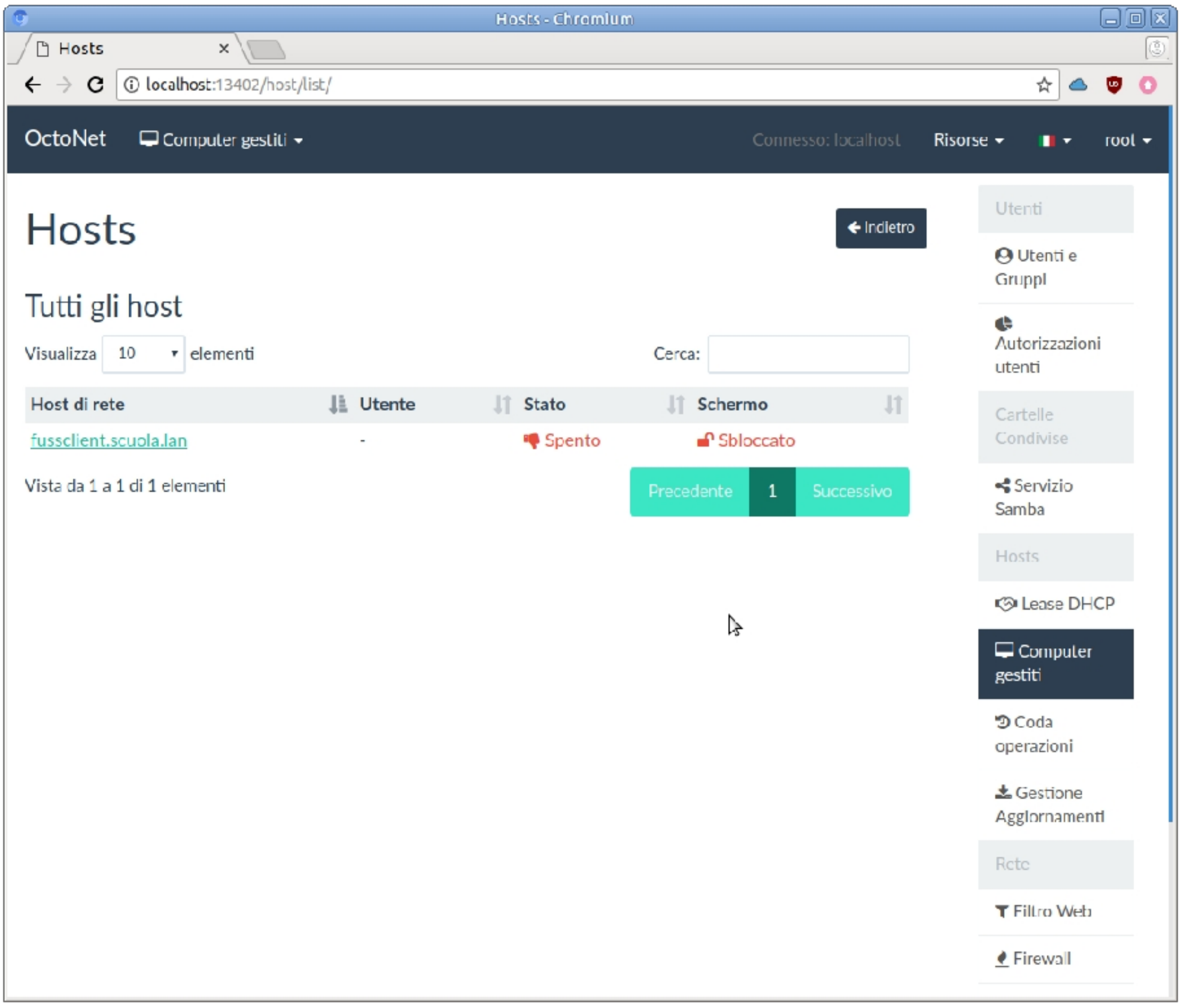


from this page you will also be able to manage present assignments by deleting them with the *Delete* button (you will be asked for confirmation in a pop-up window) or by editing them with the *Edit* button, in which case you will be taken back to the static assignment setup pages, but you will only be able to edit the MAC address and IP address fields (for name editing you need to do a delete and create from scratch).

5.3.2 Cluster management

The *Fuss Server* allows more detailed management of all clients that are registered on the server with a *join*, when you run *fuss-client -a* on them. At that stage you can ask to put the client into a *cluster*, which allows you to group groups of clients.

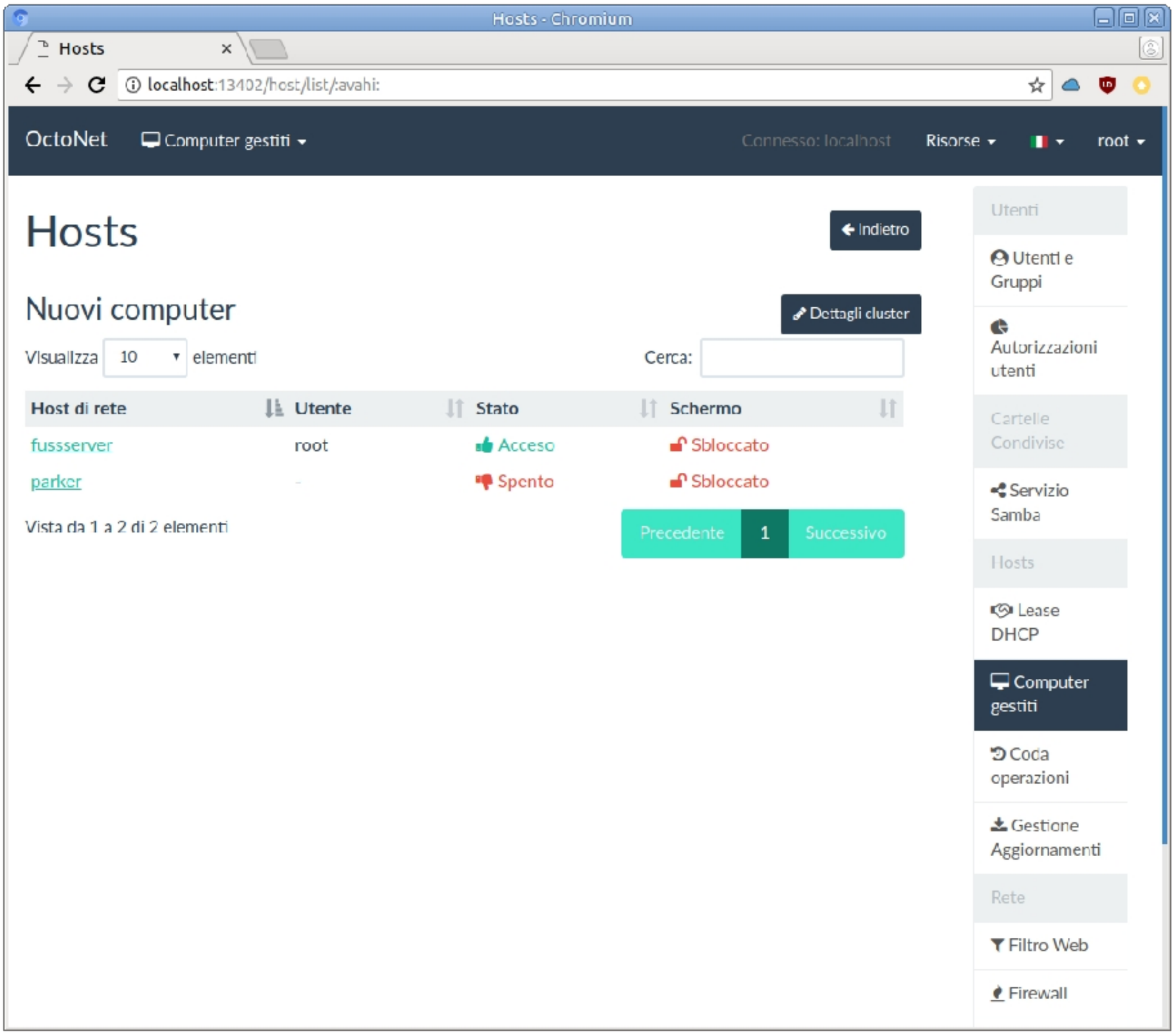
The list of computers managed by *Fuss Server* is obtained by selecting the *Managed Computers* item from the right column menu, which takes you to the Managed Hosts page, and also makes the *Managed Computers* menu available in the top bar.



The page shows the list of clients registered on the *Fuss Server* (and is initially empty) in a table where any user connected on the machine is shown, as well as the status of the machine (whether on or off) and the screen (whether locked or unlocked).

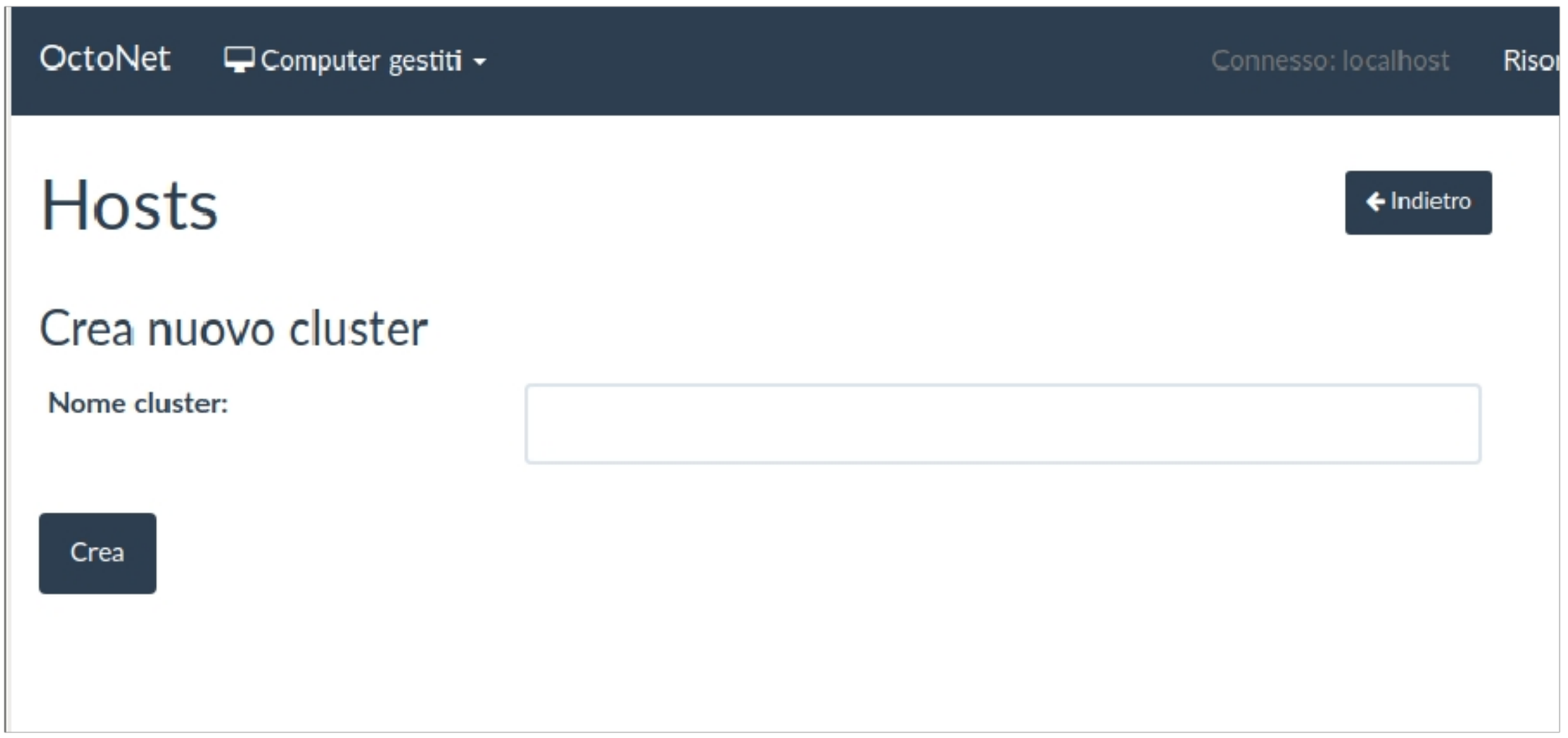
Keep in mind that the list refers to all computers that have been registered, even if those computers are no longer present. You will be able to return to the list selected from the *Computers* menu by *managing the All Hosts* item.

It is also possible to get a list of computers that have been observed on the network (thanks to the *Avahi* service) using the *New Computers* menu item, but keep in mind that this page contains a list of all computers that have been observed, not just those on the internal network on which the clients are placed.

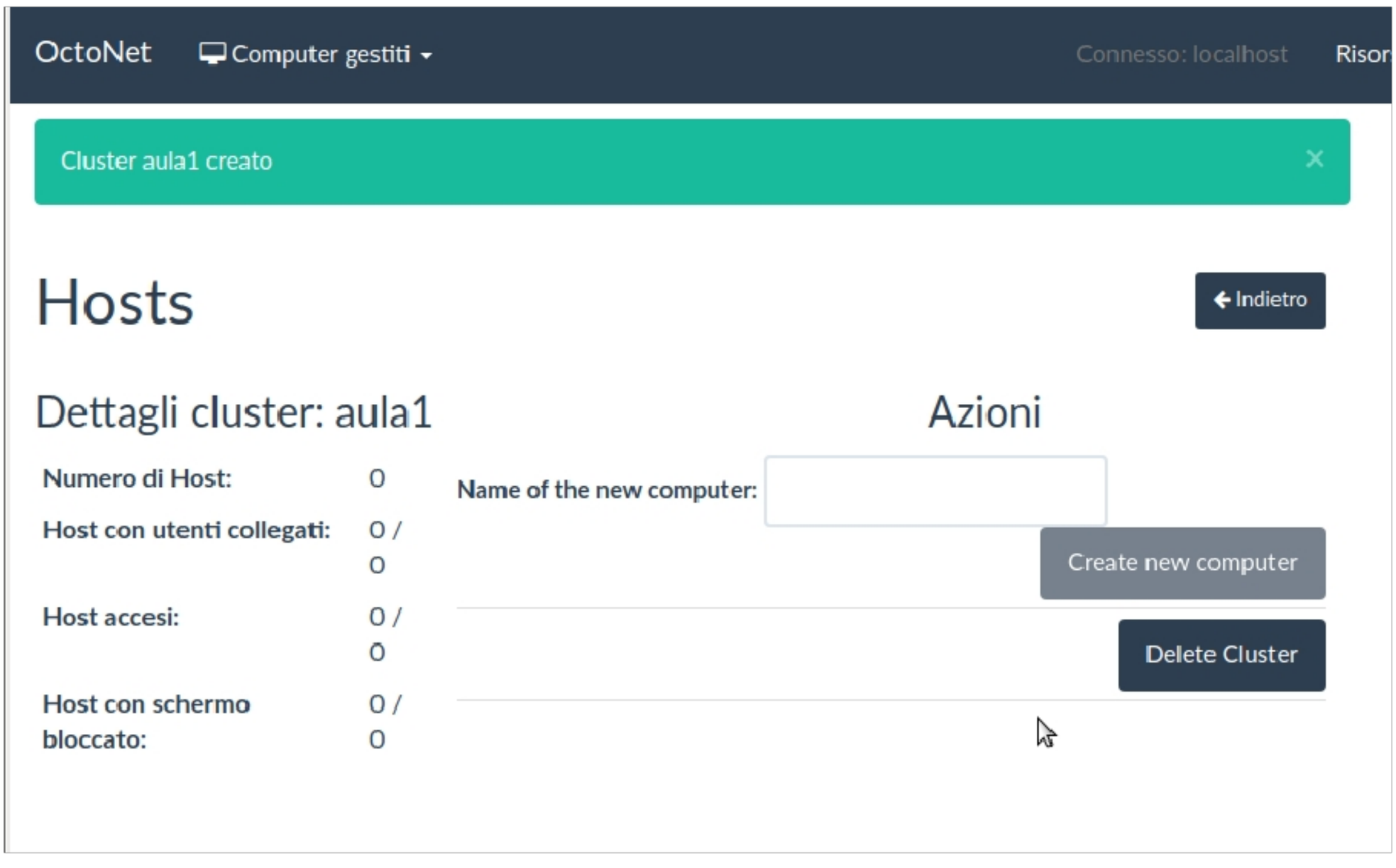


As mentioned when you run fuss-client `-a` on a client it is hooked to the server, if there is a cluster present on the server it will be automatically selected, and if there are more than one it will prompt you to choose which cluster to use. If none is present `None` will be used as the default and a cluster with that name will be automatically created.

Therefore, it is generally appropriate to create clusters on the server before running the client *join*, so that it can select which one to be included in when running `fuss-client -a`, to do this you must select from the *Managed Computers* menu in the top bar the Create *New Cluster* item which will bring in the creation page:



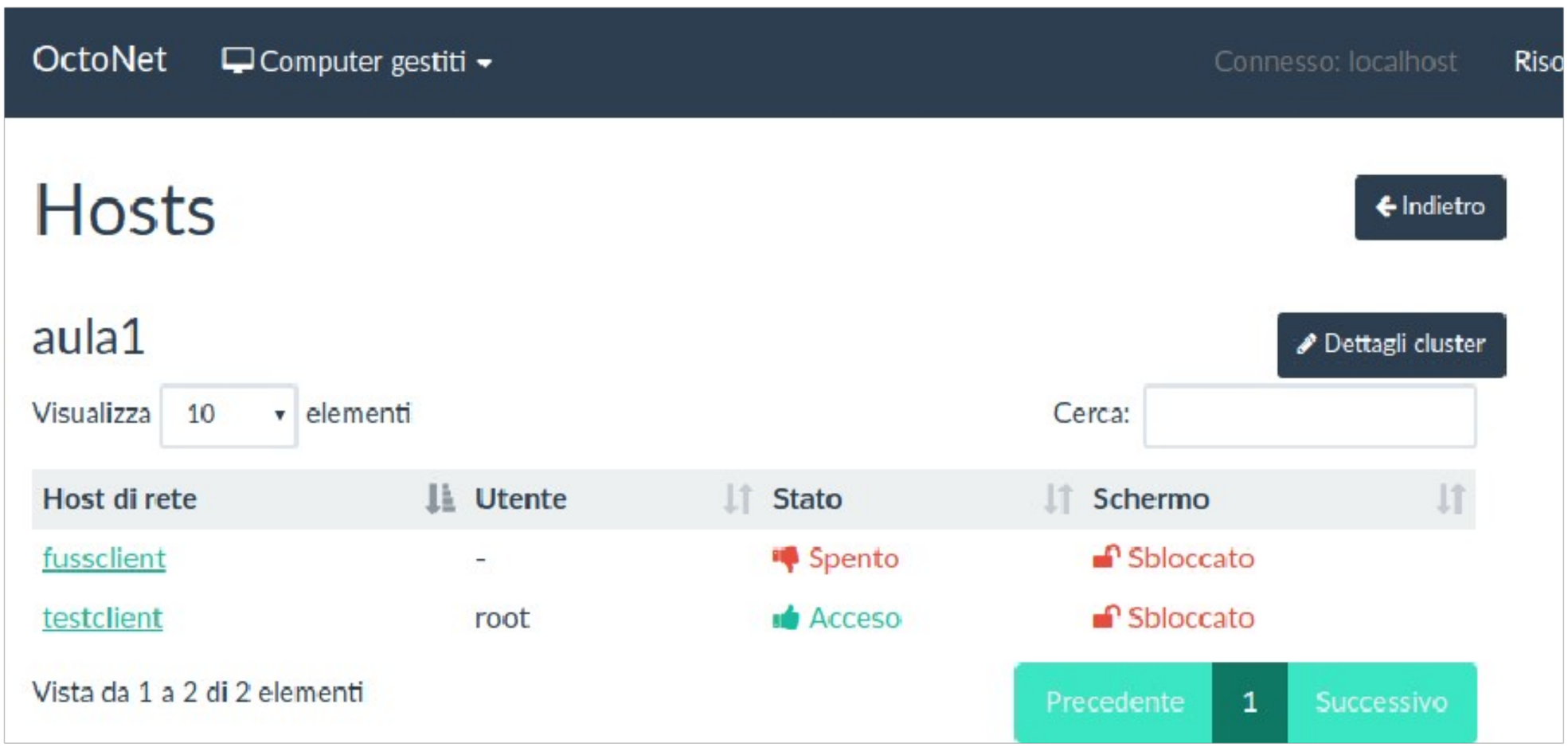
where you will be able to create a cluster by entering the name in the *Cluster Name* box, keep in mind that the name should contain no spaces and for simplicity use only lowercase letters and numbers. Once created you will be automatically redirected to the cluster management page:



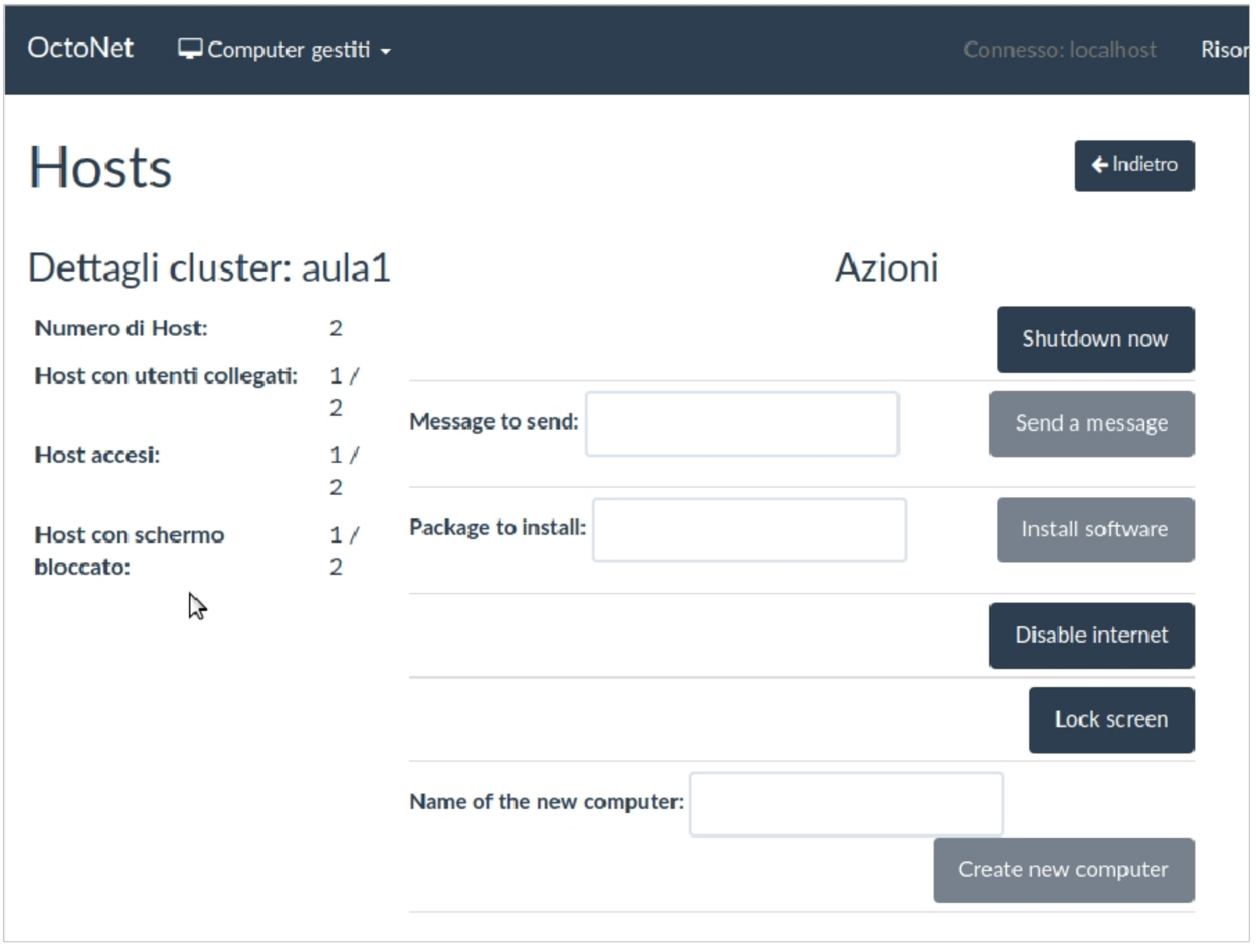
and the same will appear in the *Managed Computer* menu in the top bar, and you can select it to get to the relevant page:



Obtaining:



Pressing on the *Cluster Details* button can then take you to the cluster machine management page, from which you can perform various operations on the machines that are part of the cluster.



From this with the *Shutdown now* button you can shut down all machines in the cluster, with the *Disable internet* button you block their Internet access (an appropriate firewall rule is created), and with the *Lock* screen button you lock the screen of connected users. You can also send a message to connected users (to be entered in the *Message to send* field) with the *Send a message* button and indicate a package to be installed (to be entered in the *Package to install* field) with the *Install software* button.

Finally, a new client can be placed in the cluster using the *Create new computer* button, writing its name in the *Name of the new computer* field.

5.3.3 Manual cluster management

Cluster data are maintained on the *Fuss Server* in the file `/etc/clusters`, the format of which is in the form of one line per cluster of machines, with fields separated by spacings, in which the first field, the one at the beginning of the line, indicates the name of the cluster, and the subsequent fields the names of the clients that are part of it.

Keep in mind that in the ordinary connection to the server, clients are identified only by hostname (with the single name, not the full FQDN), but this is the case with newer versions of the client, which have introduced support for name normalization and the ability to change a machine's hostname on the fly before connecting.

If you have to intervene manually on this file you need to have some caution, in fact its contents vie- read by `octofussd` at startup, and updated consistently as long as you use *OctoNet* or add clients with `fuss-client`, but if you operate manually on `/etc/clusters` you need to force the re-read with `service octofussd restart`.

In case you want to create the file manually you can use the data collected thanks to the DHCP service, but for this it is necessary that all the PCs that are to be included in the cluster are turned on. If this is the case, it is possible to display all powered-on machines on the screen with the command:

```
host -l "domainname.local"
```

and from this list you can create the `/etc/clusters` file by running (again from the server console) the command:

```
host -l "domainname.local" \
| cut -d "." -f 1 \
| head -n -1 \
| sort \
| tr '\n' ' ' >> /etc/clusters
```

Alternatively, we can extract, rather than the client names, the IPs delivered by the DHCP server (useful when the client locations do not yet have `fuss-client` installed, which configures `dhclient` to have the client names on the DNS) in this way:

```
grep lease /var/lib/dhcp/dhcpd.leases \
| head -n -8 \
| cut -d " " -f 2 \
| sort | uniq \
| tr '\n' ' ' >> /etc/clusters
```

You can use the cluster definition data directly from the server console with the command:

```
cssh nomecluster
```

or from a client location, I must, however, first connect to the server with:

```
ssh -X root@server
```

or:

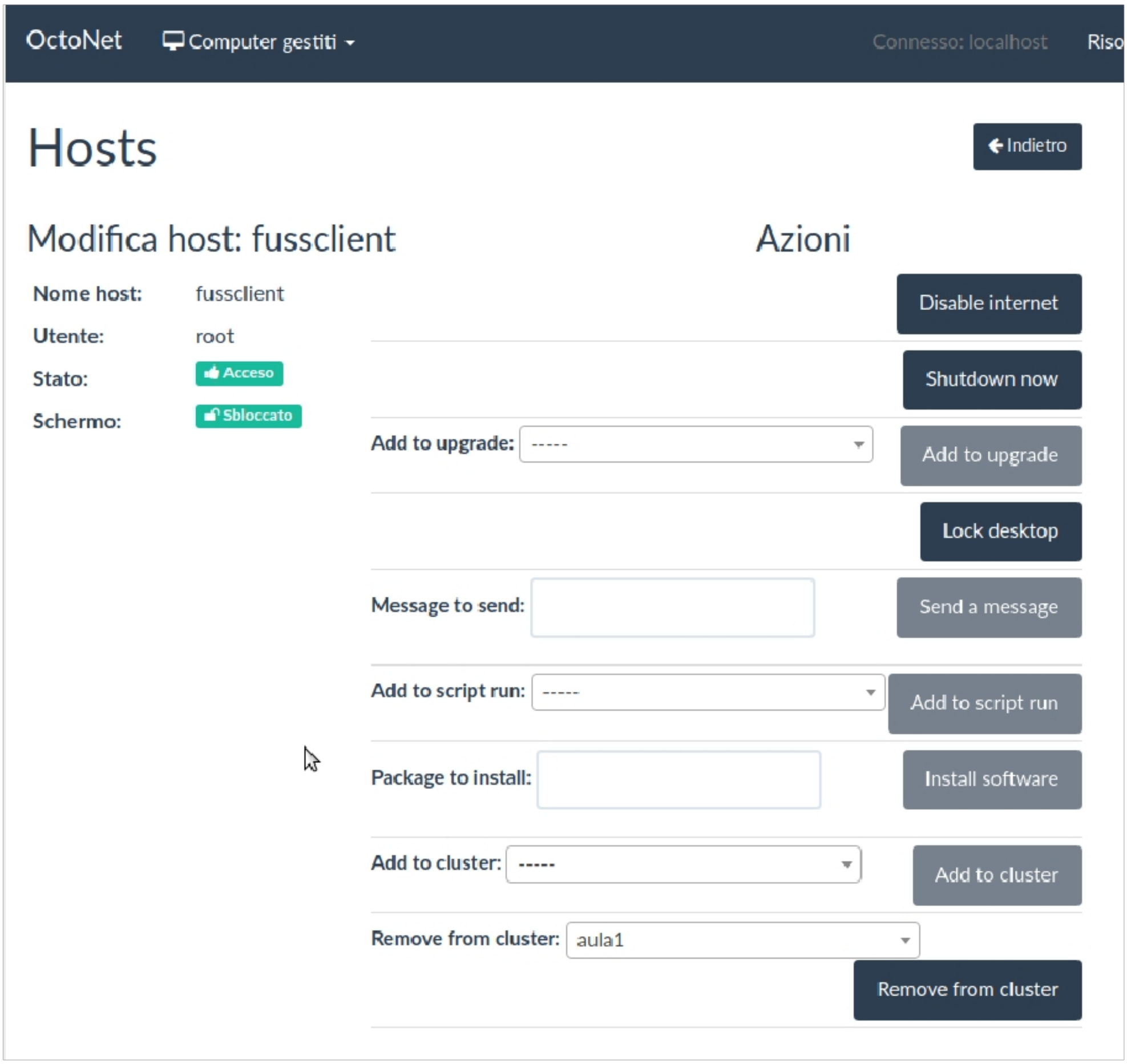
```
ssh -X server -l root
```

And start cssh:

```
cssh nomecluster
```

5.3.4 Host management

In addition to the general management of clients that are part of a cluster, operations can be scheduled for individual machines. These operations can be accessed by clicking on a machine's link from the *All Hosts* page (or from that of a cluster of which the machine is a part), which takes you to the requested host's page:



The page shows the possible *Actions* on the right-hand side; some of these (*Shutdown now*, *Disable internet*, *Lock desktop*, *Send a message*, *Install software*) are the same as those already seen for machines in a cluster in *Cluster Management*; to these are added the ability to insert the machine into a cluster (to be selected from the *Add to cluster drop-down menu*) with the *Add to cluster* button and the ability to remove it from a cluster with (to be selected from the *Remove* from cluster drop-down menu) with the *Remove from cluster* button.

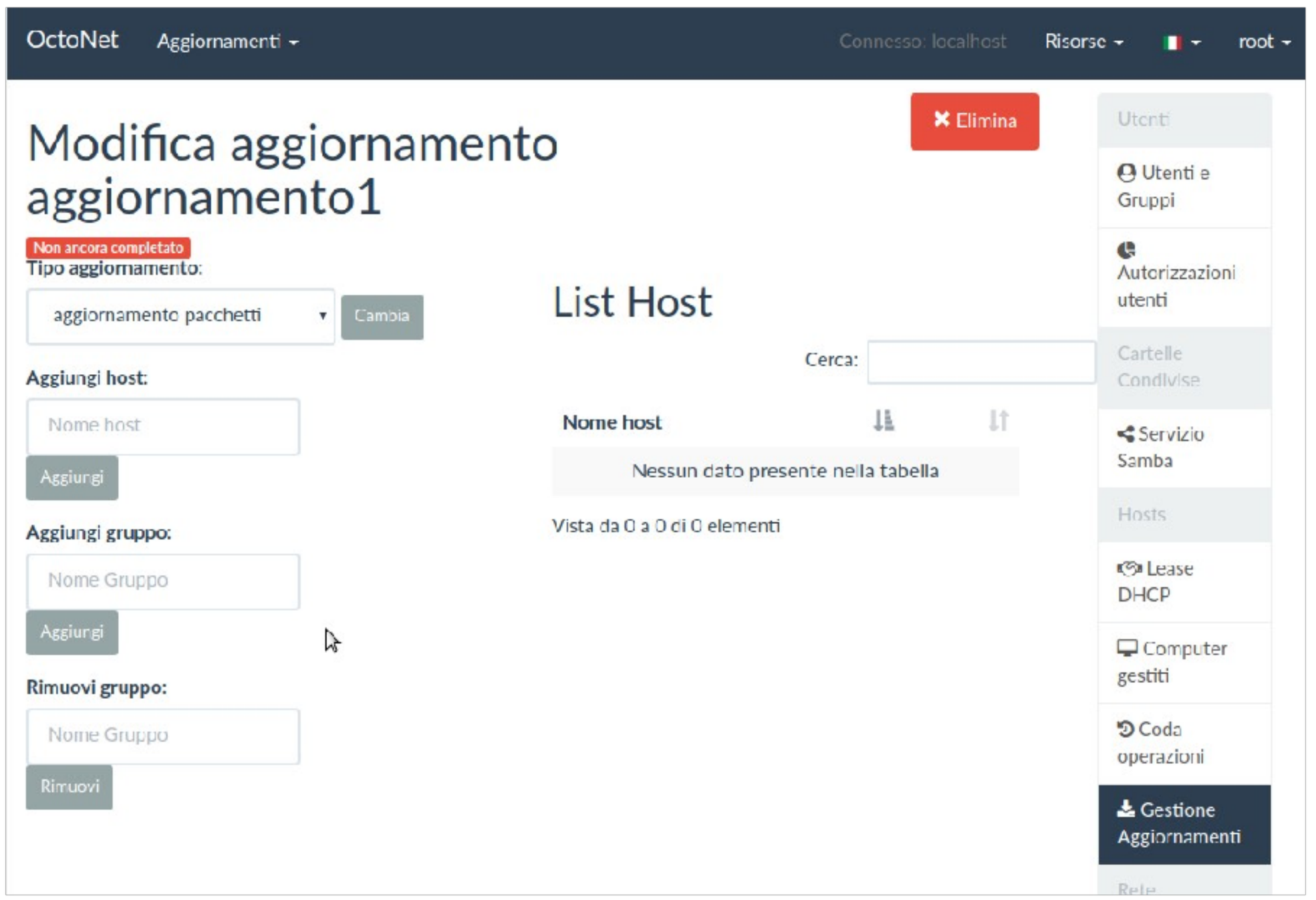
Finally, it is possible to add the machine to a planned upgrade (which must be created earlier, see *Upgrade Management*) by selecting it from the *Add* to upgrade drop-down menu with the *Add to upgrade* button, or to schedule the execution of one of the management scripts placed on the platform (also must be created earlier, see *Script management*) again to be selected from the *Add* to script run drop-down menu with the *Add to script run* button.

5.3.5 Update management

For managing updates to machines connected to the *Fuss Server,* update jobs can be set up using the *Update Management* item from the right operations menu.



This takes you to the page listing the jobs you have set up, from which you can set up a new update in the *Create New Update* section by indicating a name for it in the text box and clicking on the adjacent *Create* button, which will take us to the page for setting it up.



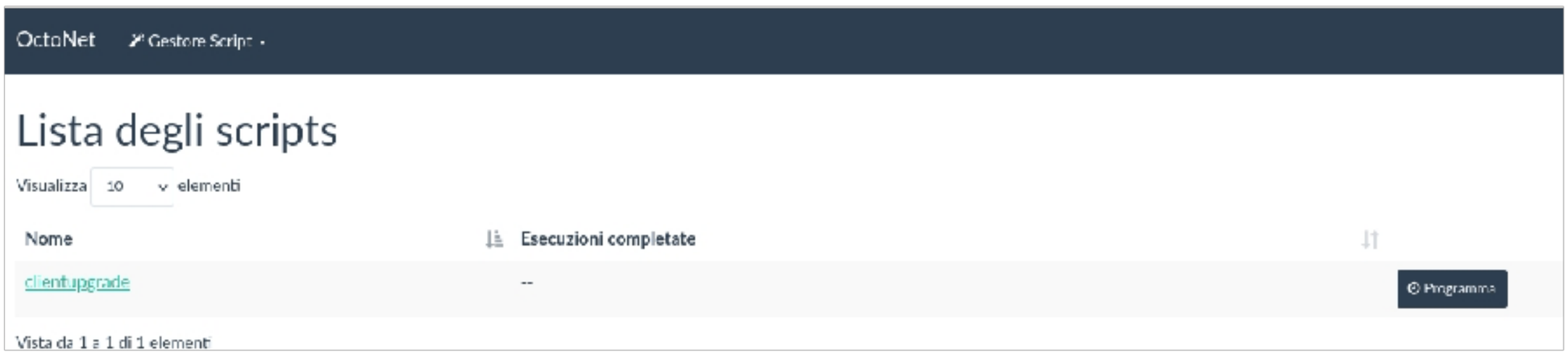
From the page, you will be able to select the type of upgrade from the Upgrade *Type* box (with the two possibilities *Package Upgrade* and *Distribution Upgrade* corresponding t o running `apt-get upgrade` and `apt-get dist-upgrade`) and select the machines to be included in the upgrade either individually from the *Add Host* box or by cluster from the *Add Group* box.

Until at least one machine is entered into the update, the green *Program* button does not appear, allowing you to schedule the operation, which instead can be canceled at any time with the red *Delete button. Once* a machine is entered into the update it will appear in the list on the right, flanked by a *Remove* button that allows you to remove it from the update.

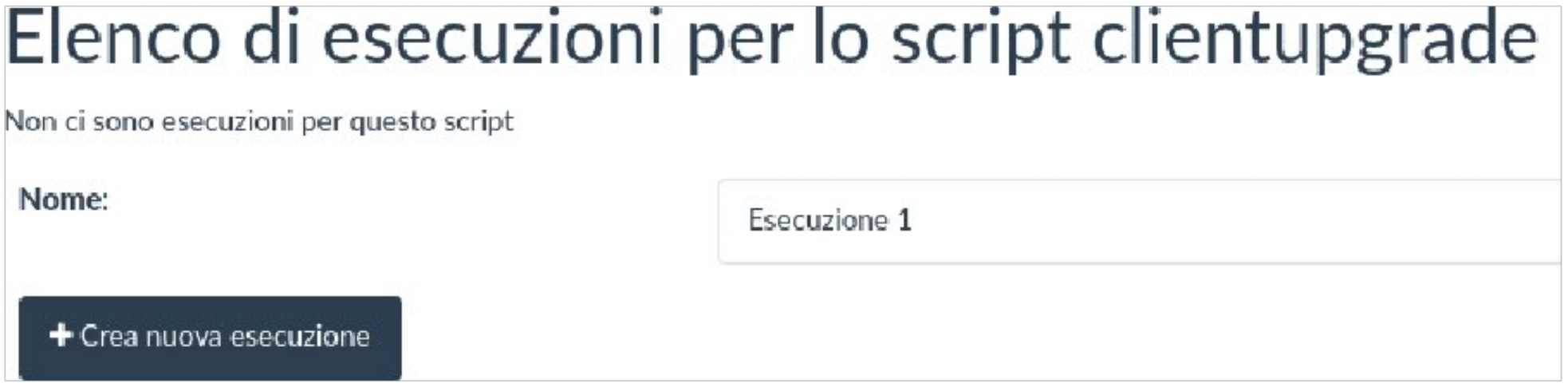
When you have finished entering the machines you want in the update you can program it with the button *Program*, from then on it will no longer be editable.

5.3.6 Script management

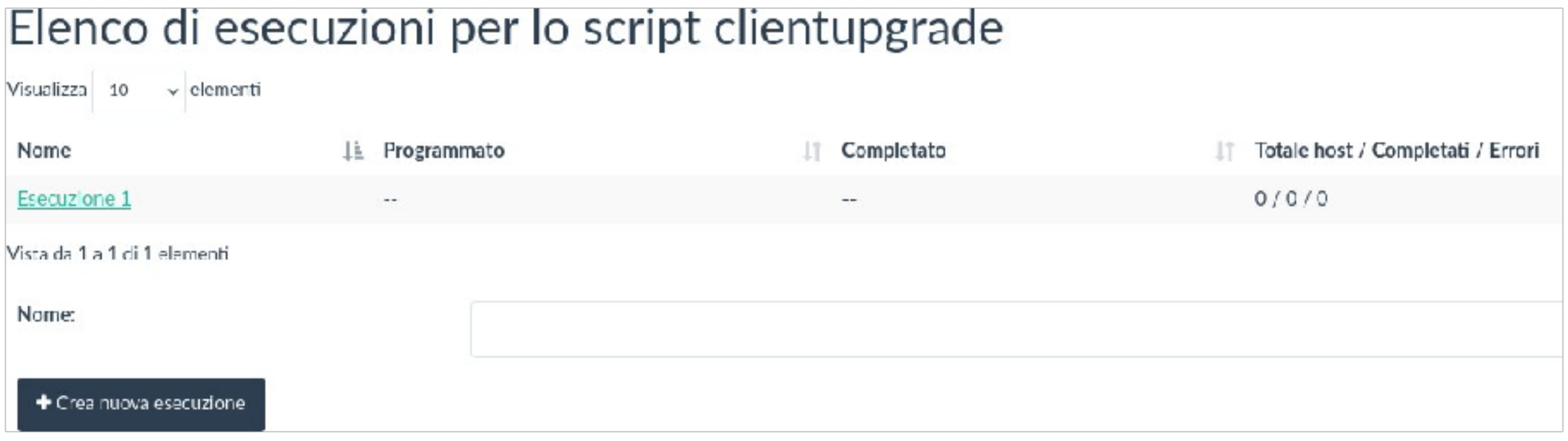
From the main page of **Octonet** click at the bottom right on the `Script Manager` item . You are on the page with the `List of scripts` .



Click on the `Program` button located to the right of the chosen script.

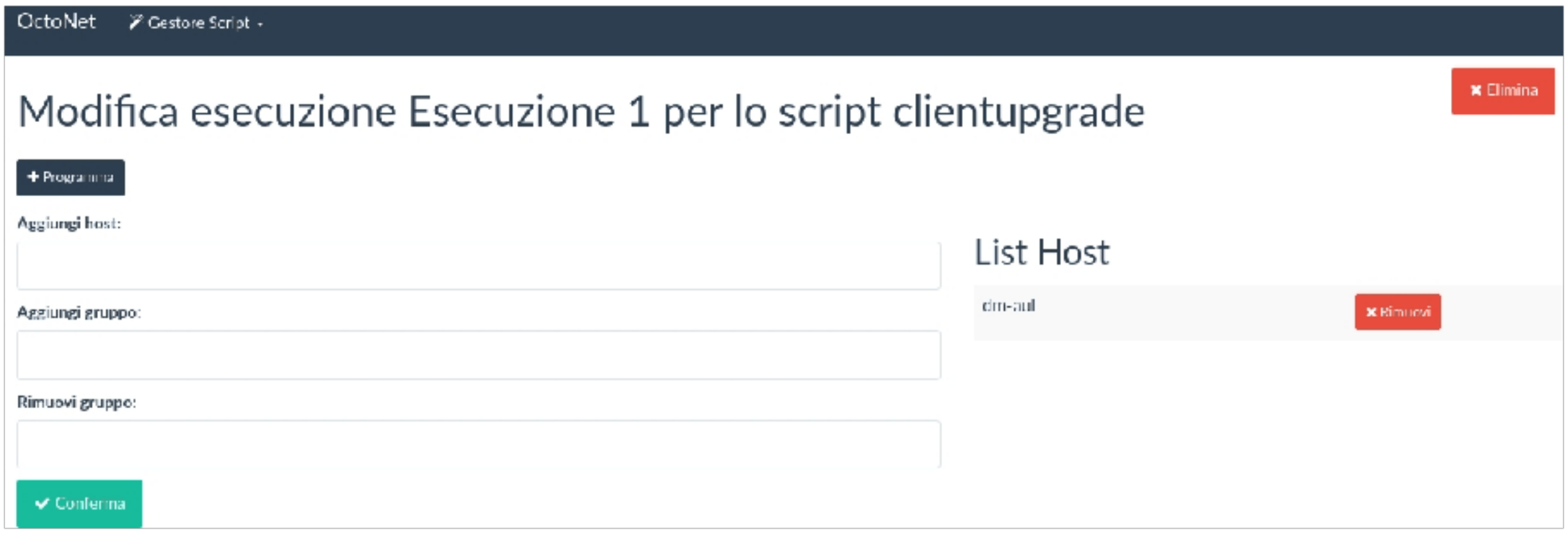


After assigning a `Name` click on the `Create a new Execution` button . Click on the name of the newly created Execution.



At this point hosts or groups (clusters) should be added by entering them in the appropriate fields and clicking on the `Confirm` button each time .

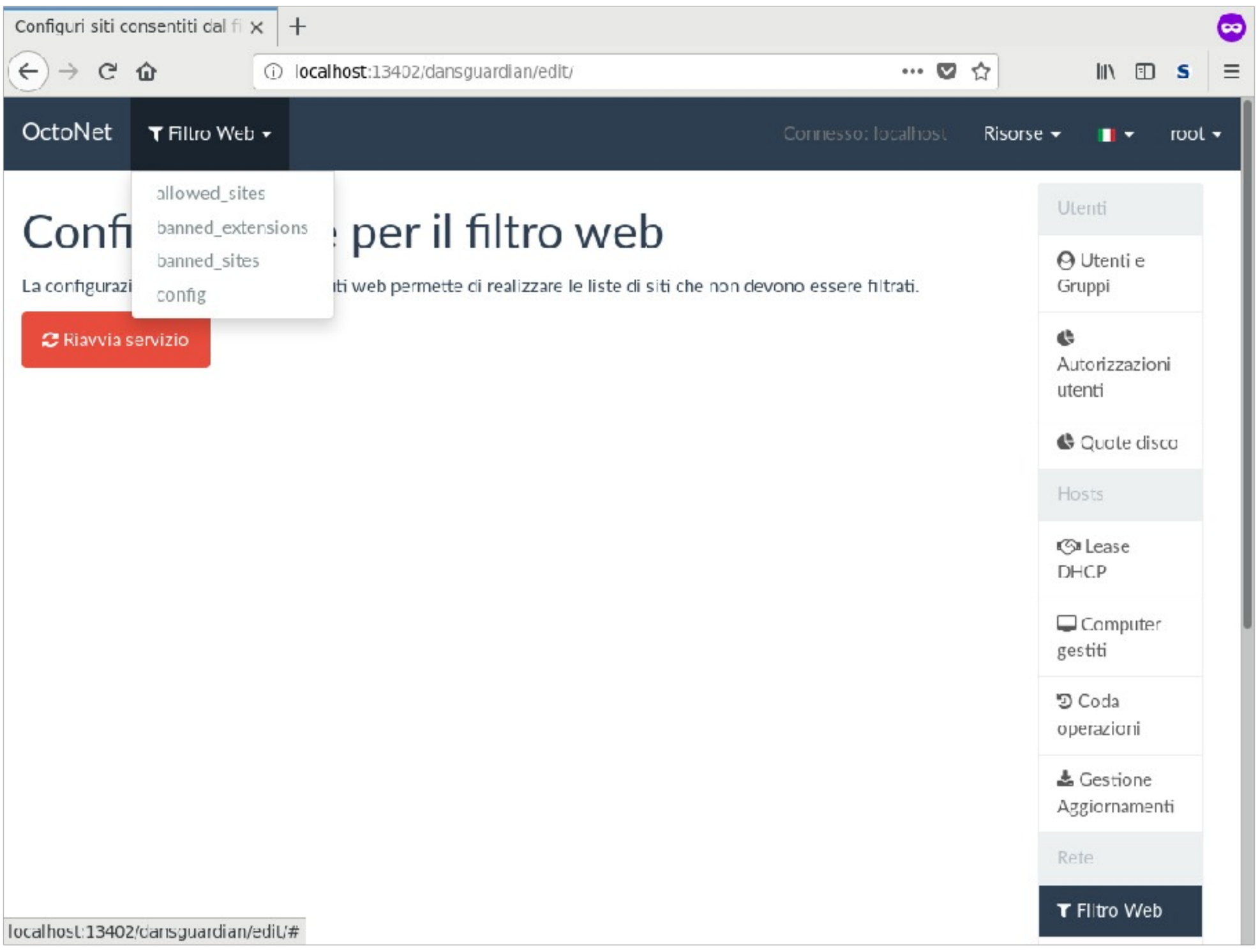
Finally you launch the script by clicking on the black `Program` button . Keep in mind that the script is not launched instantly but usually spends a few minutes.



When the execution is finished, it can be deleted by clicking on the red `Delete` button.

5.4 Filter management web

Through the *Network → Web Filter* item in the sidebar, you can access the content filter management page for browsing, enabling its menu in the top bar.

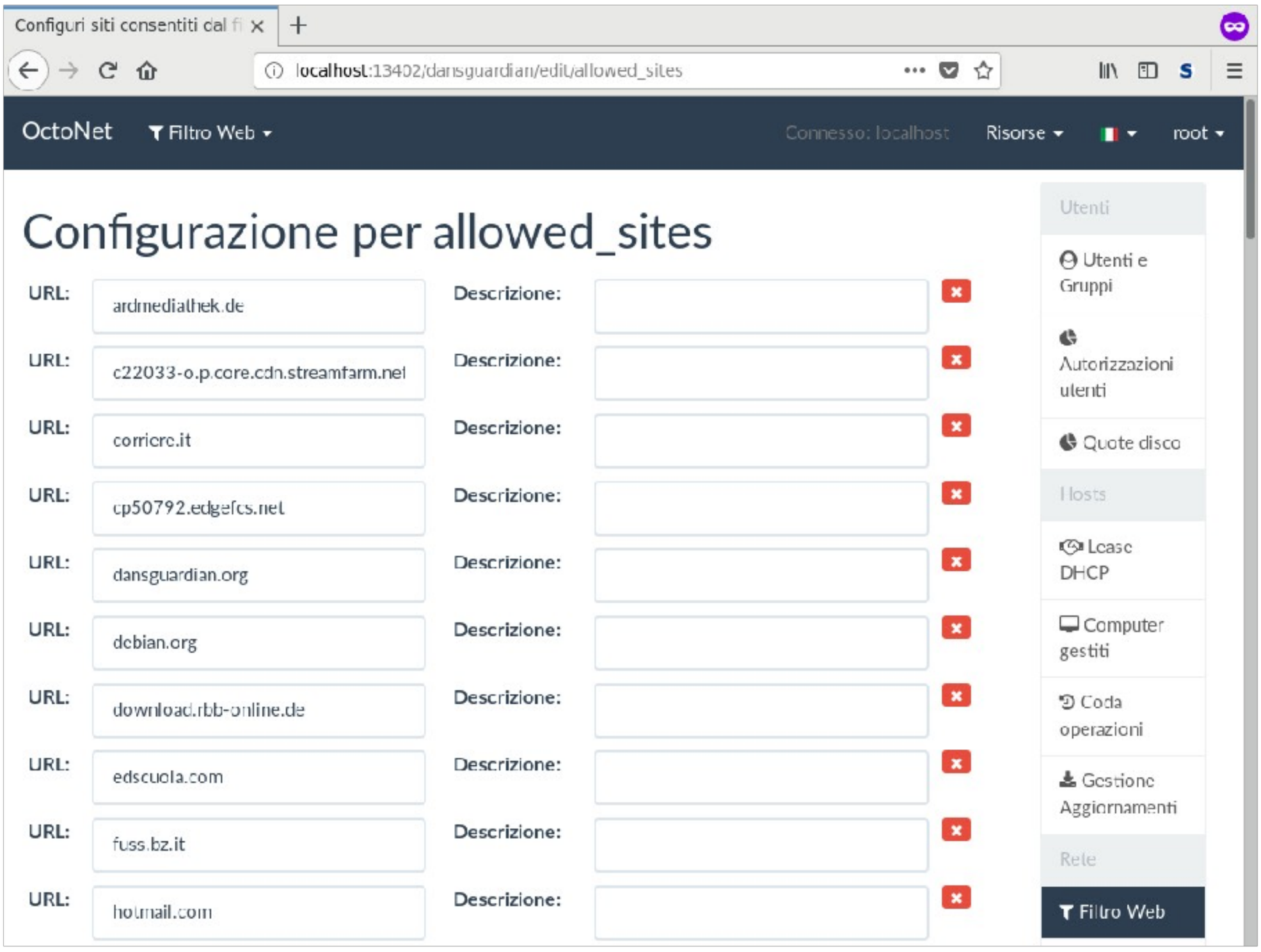


The menu items present correspond to the program configuration files that manage t h e navigation rules, documented in detail in the appropriate *e2guardian (content filter)* section of the guide.

The various pages contain a list of entries, for each of which there is a *Description* field through which to provide comments about the entry and why it was entered.

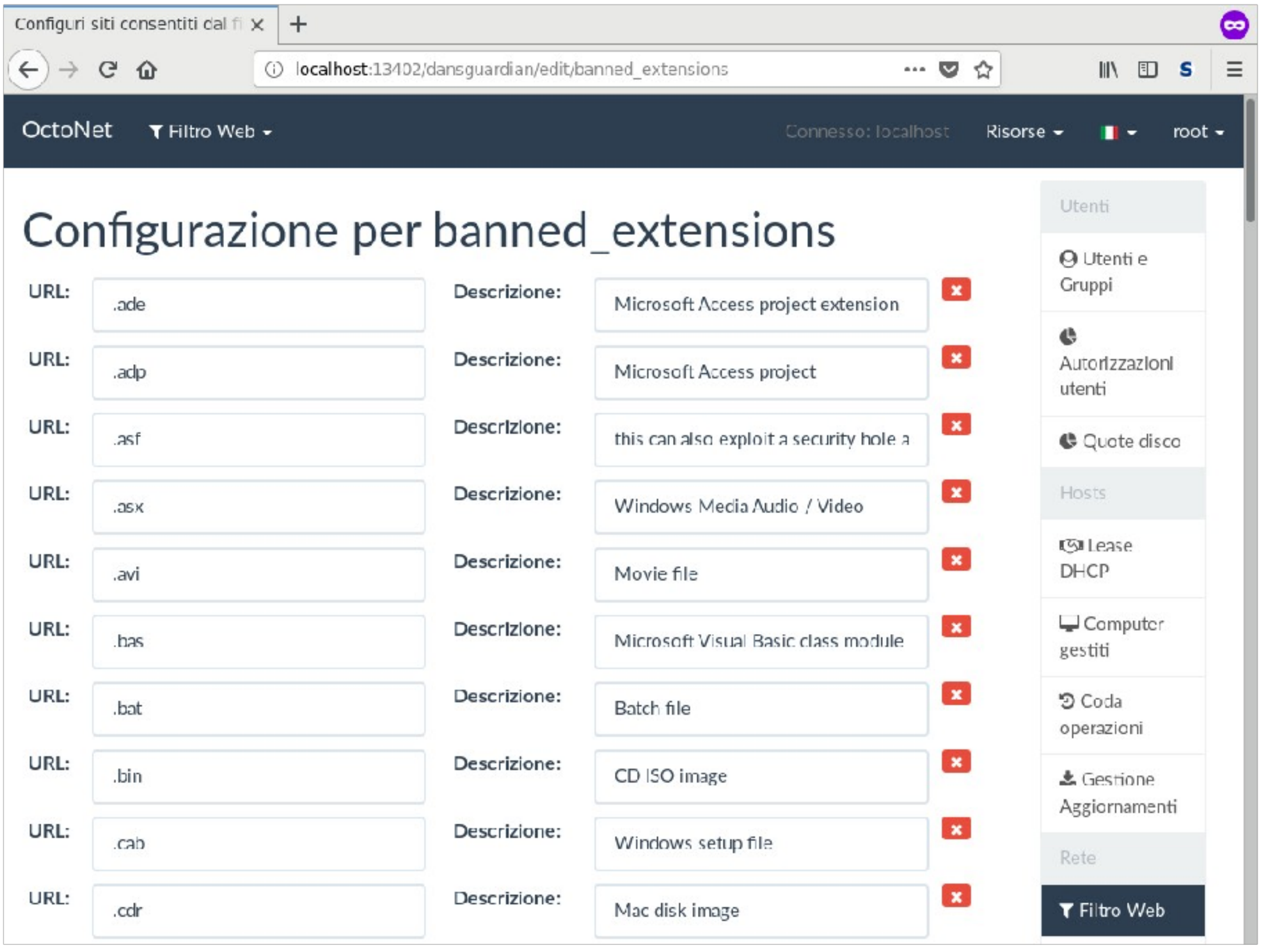
The first menu item, *allowed_sites* allows you to manage the list of domains that are always allowed to access, regardless of imposed bans.

The corresponding file is `/etc/fuss-server/content-filter-allowed-sites`.



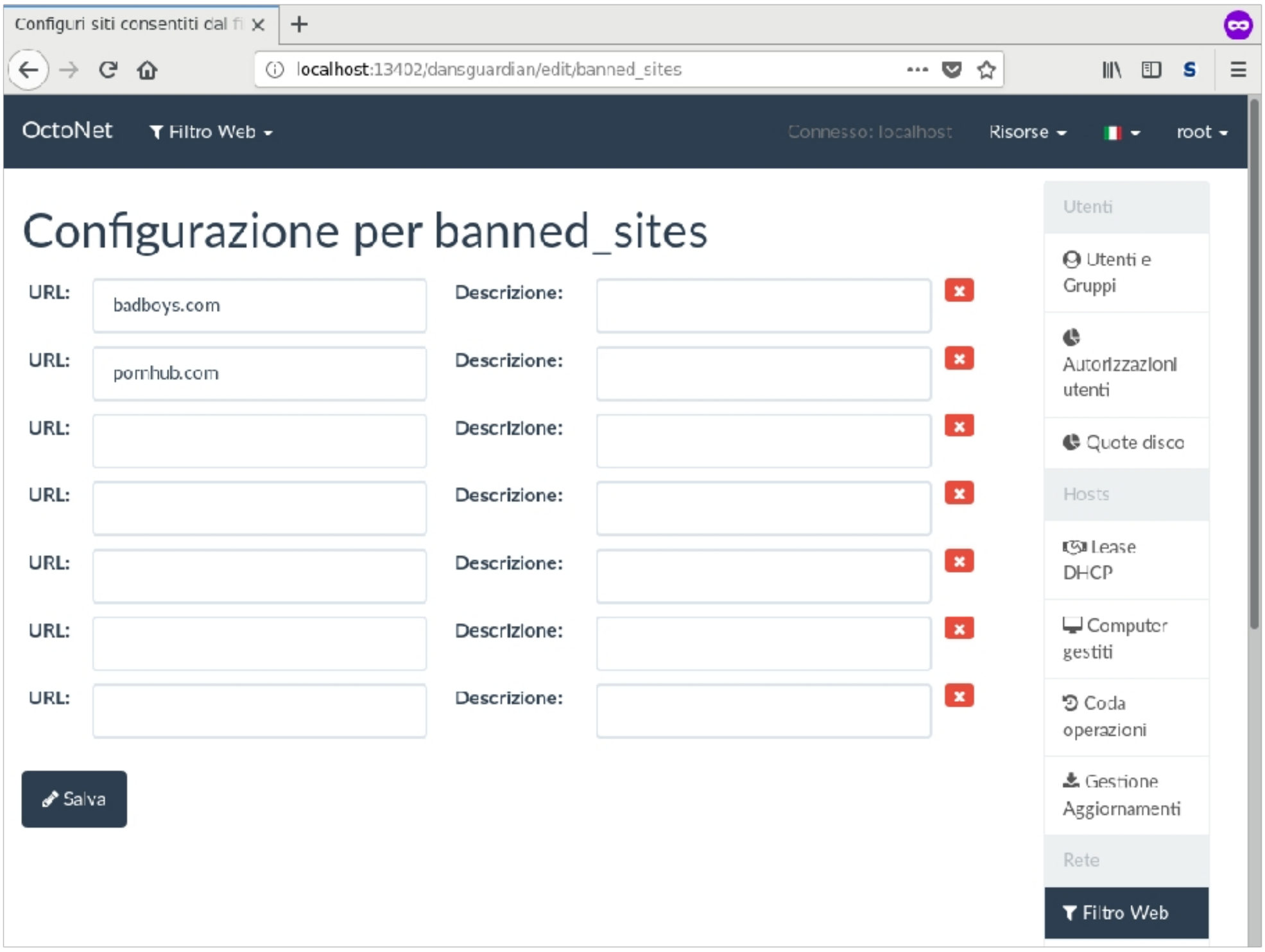
banned_extensions is a list of file extensions to which access is prohibited.

The corresponding file is `/etc/dansguardian/lists/bannedextensionlist`.



banned_sites is a list of domains to which access is always prohibited.

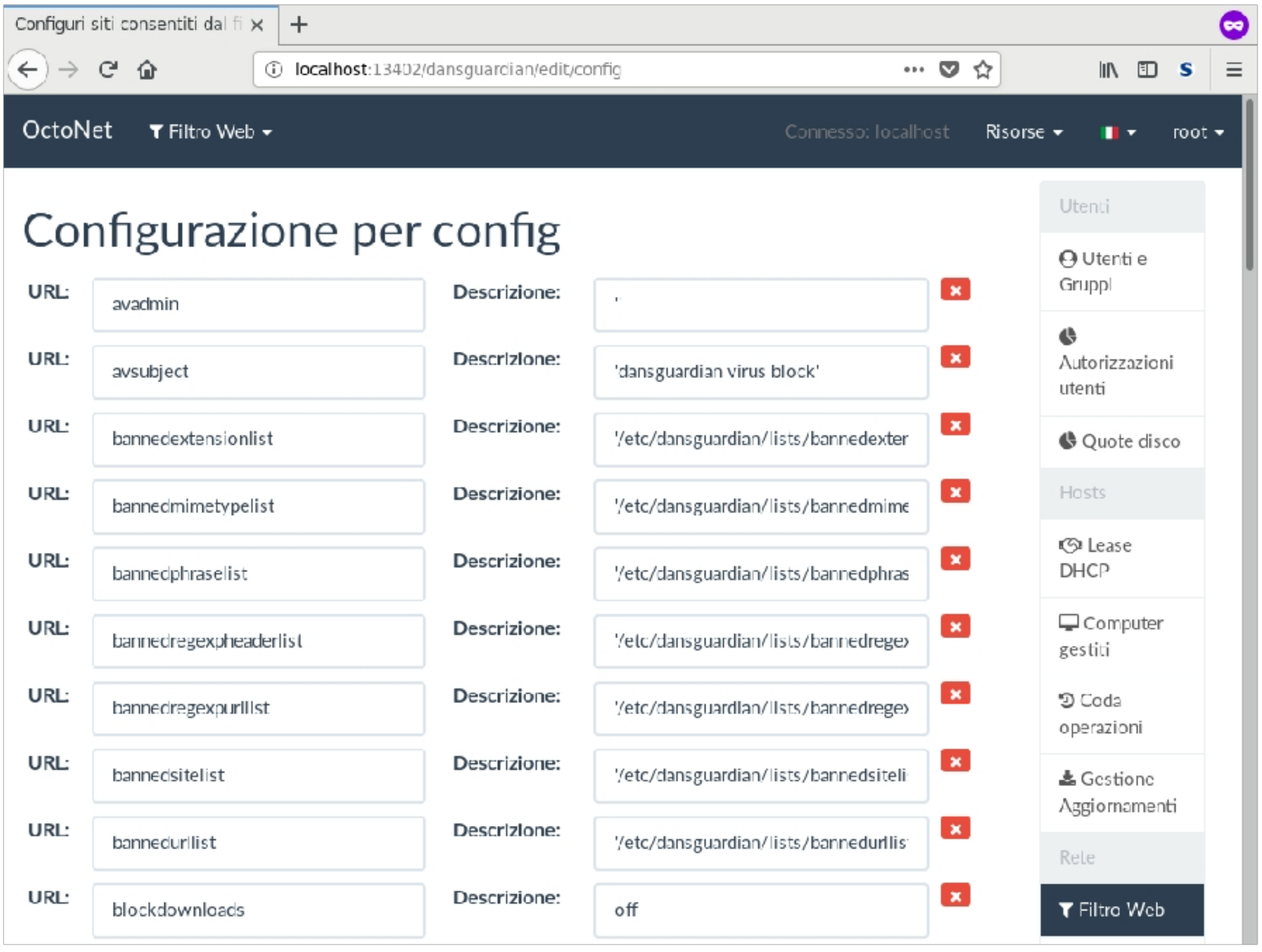
The corresponding file is `/etc/dansguardian/lists/bannedsitelist`.



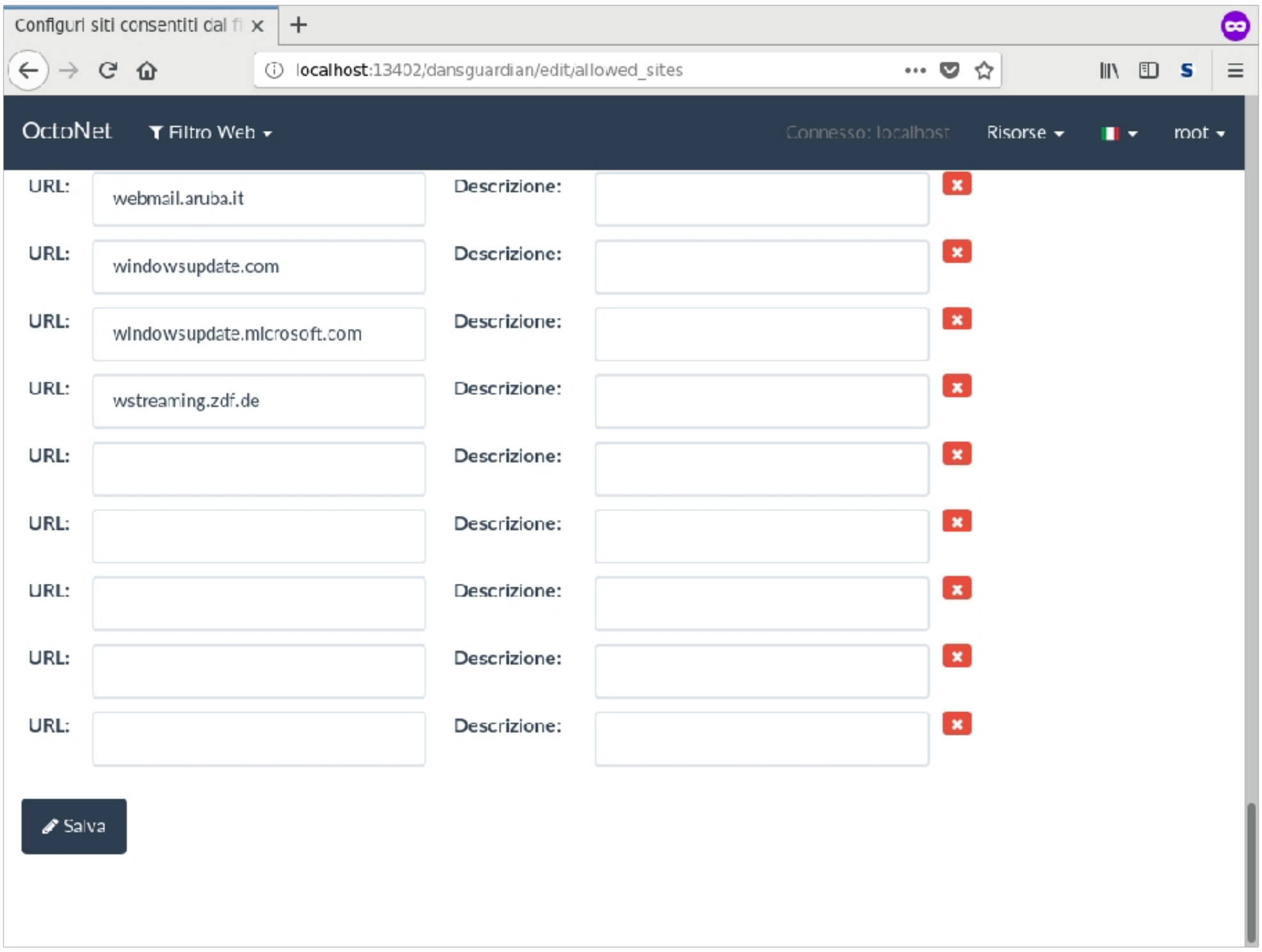
And finally, *config* allows you to change the configuration of dansguardian itself; in this case, the field *Description* contains the value of the corresponding configuration parameter.

The corresponding file is

`/etc/dansguardian/dansguardianf1.conf`.

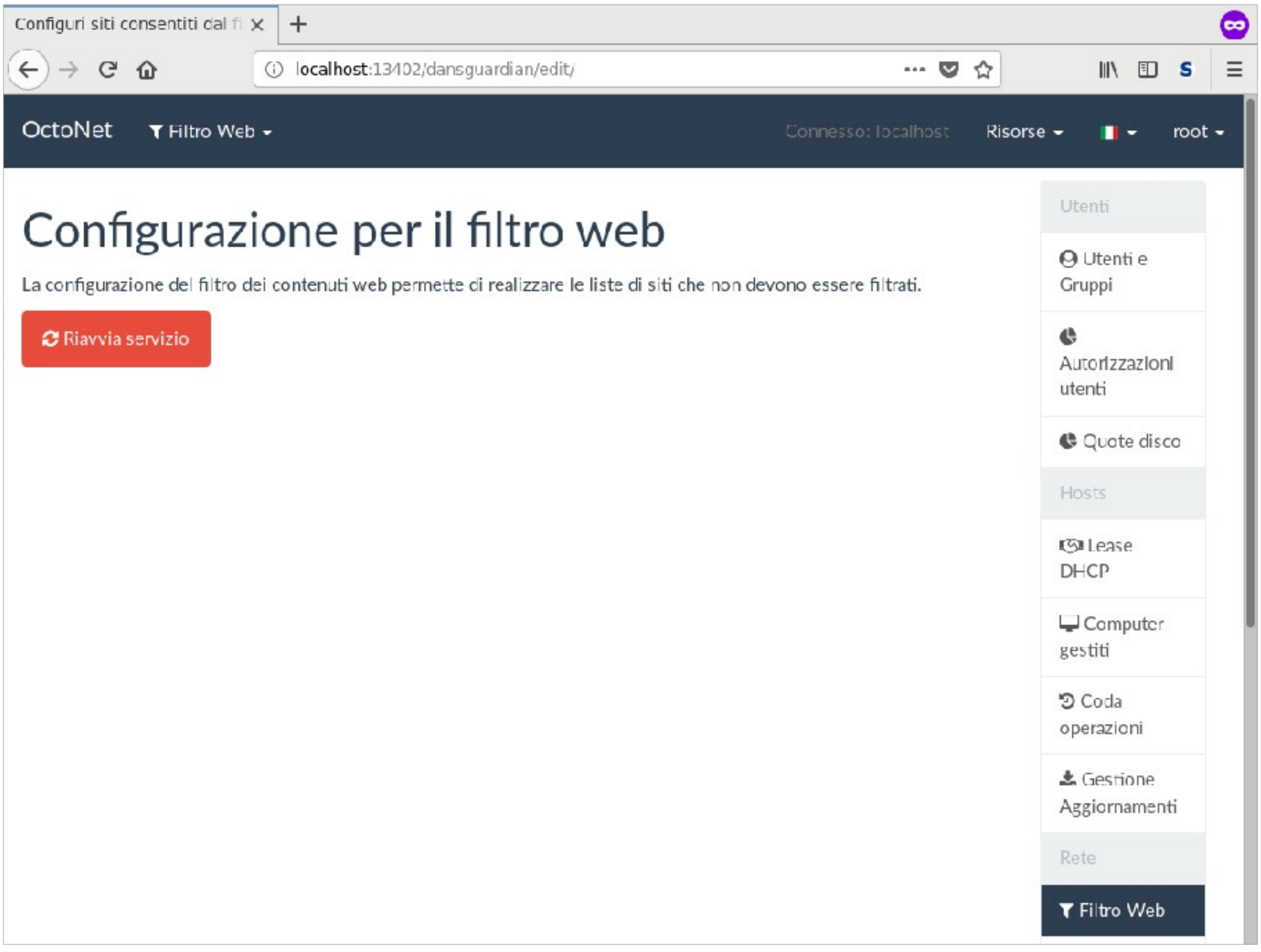

Configuri siti consentiti dal fi
localhost:13402/dansguardian/edit/config
OctoNet
Filtro Web
Connesso: localhost
Risorse
root
Configurazione per config
URL: avadmin
Descrizione:
URL: avsubject
Descrizione: 'dansguardian virus block'
URL: bannedextensionlist
Descrizione: '/etc/dansguardian/lists/bannedexter
URL: bannedmimetypelist
Descrizione: '/etc/dansguardian/lists/bannedmime
URL: bannedphraselist
Descrizione: '/etc/dansguardian/lists/bannedphras
URL: bannedregexpheaderlist
Descrizione: '/etc/dansguardian/lists/bannedrege
URL: bannedregexpurllist
Descrizione: '/etc/dansguardian/lists/bannedrege
URL: bannedsitelist
Descrizione: '/etc/dansguardian/lists/bannedsiteli
URL: bannedurllist
Descrizione: '/etc/dansguardian/lists/bannedurllis
URL: blockdownloads
Descrizione: off
Utenti
Utenti e Gruppi
Autorizzazioni utenti
Quote disco
Hosts
Lease DHCP
Computer gestiti
Coda operazioni
Gestione Aggiornamenti
Rete
Filtro Web

5.4.1 Changes to web filters



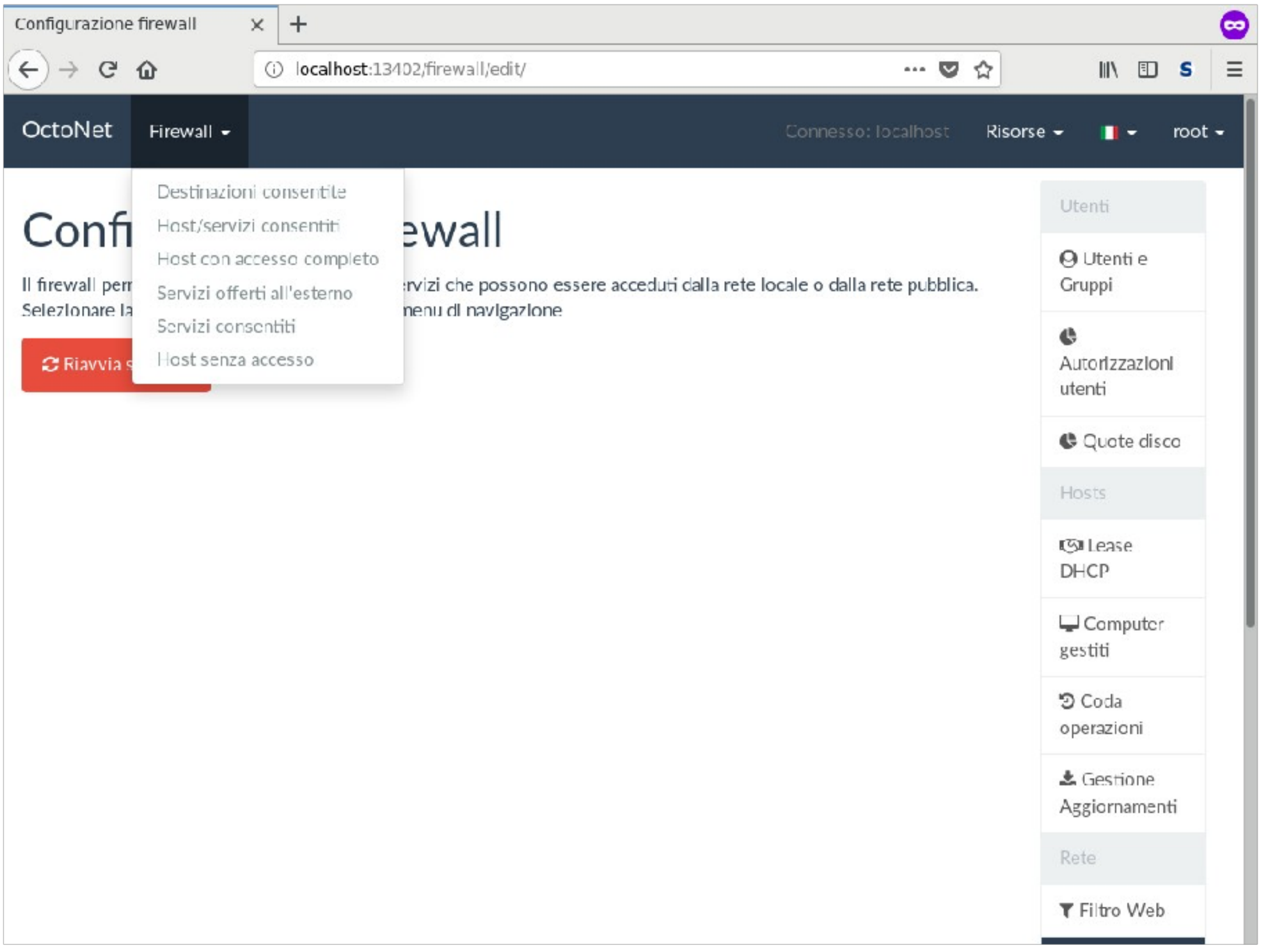
The fields on the pages just seen can be edited, or emptied by pressing the corresponding red x key; new entries can be added in the five blank lines at the bottom of the page.

For changes to be written to the configuration files, it is then necessary to press the *Save* button, and eventually restart the service from the main page of this section for them to become active.



5.5 Management firewall

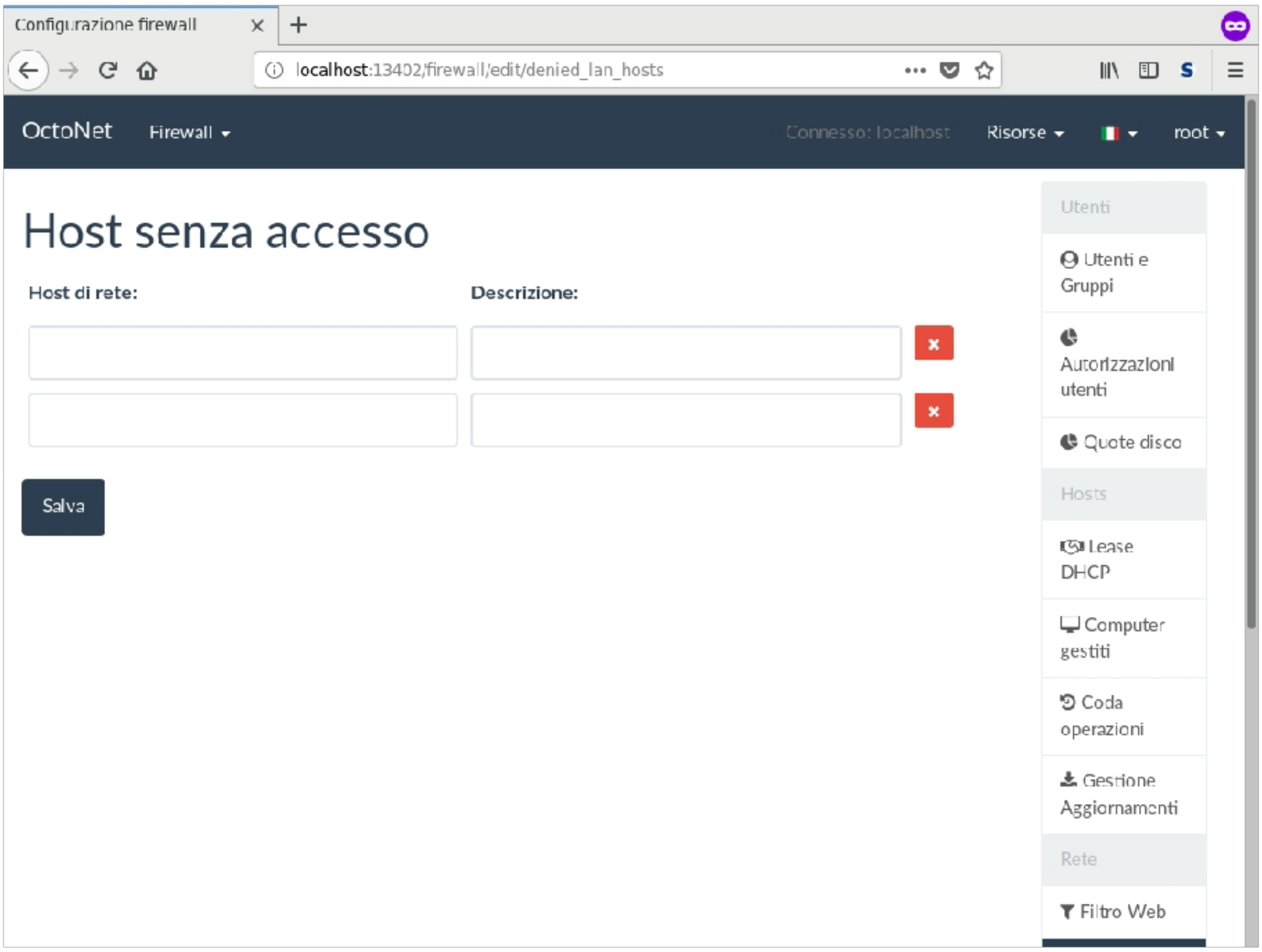
Through the *Network* → *Firewall* item in the sidebar, the firewall management page is accessed by enabling its menu in the top bar.



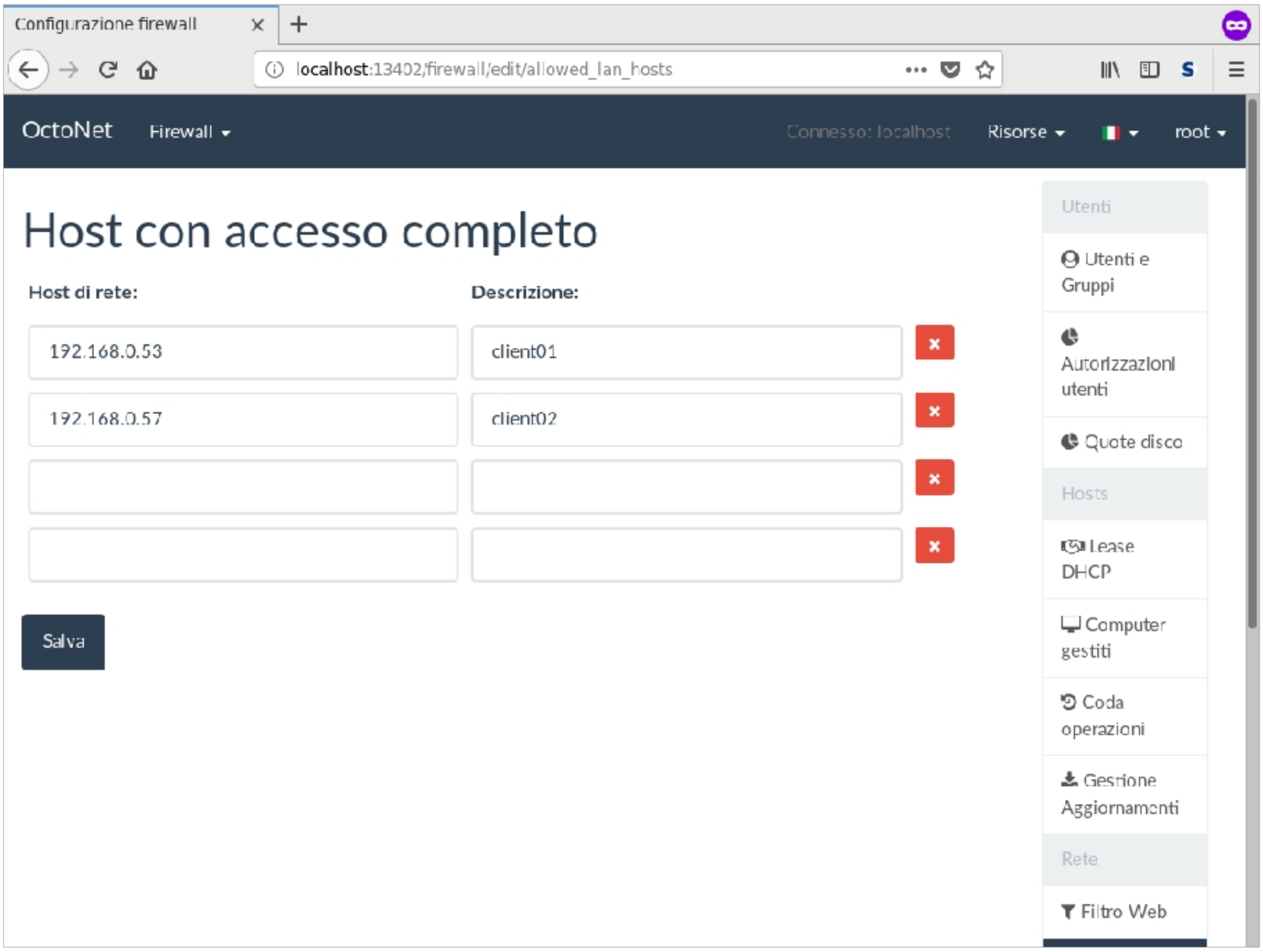
The menu items present correspond to the configuration files of the program that manages t h e browsing rules, documented in detail in the *Firewall* section of the guide.

The various pages contain a list of entries, for each of which there is a *Description* field through which to provide comments about the entry and why it was entered.

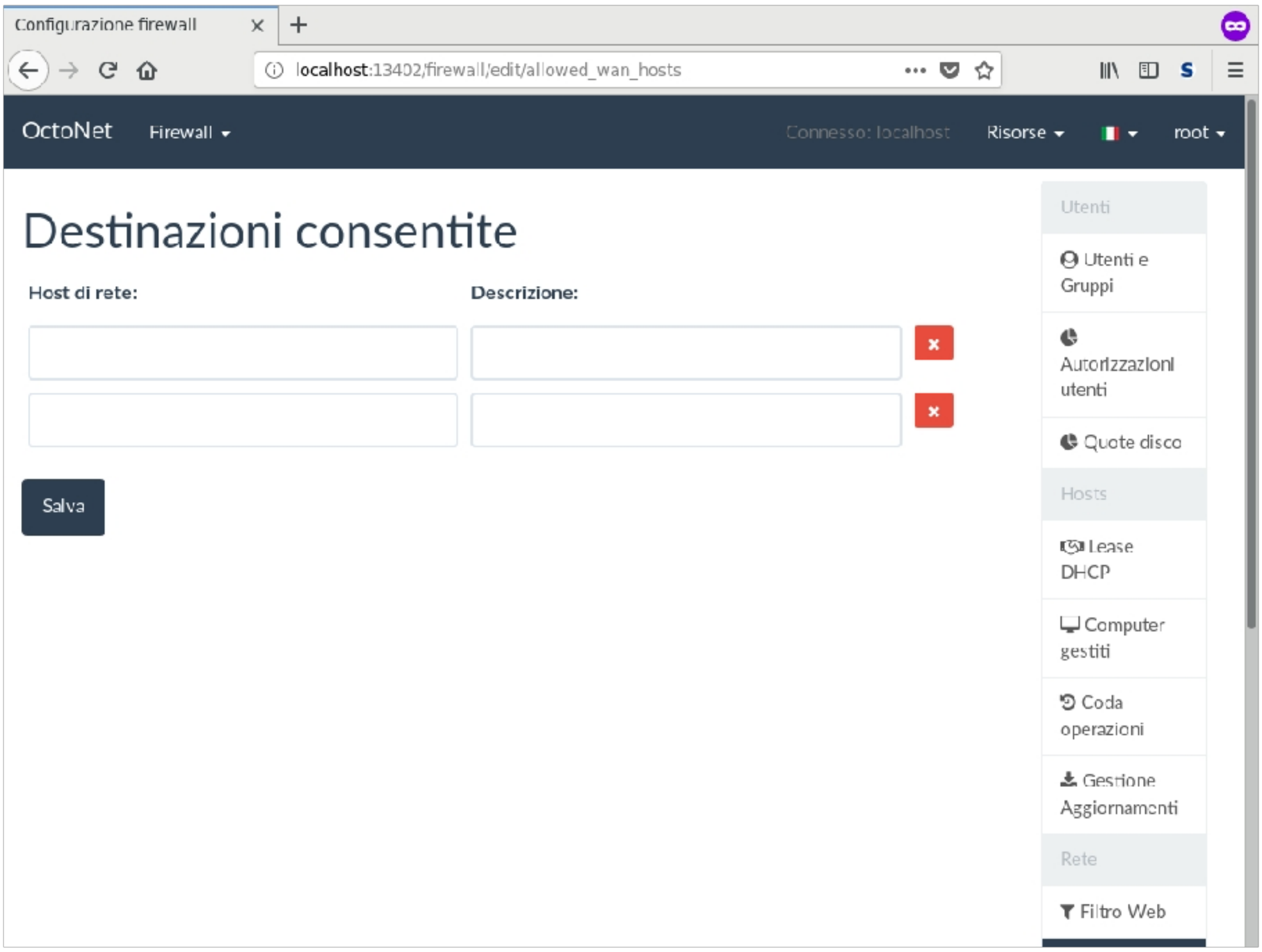
Host without access corresponds to the file `/etc/fuss-server/firewall-denied-lan-hosts`



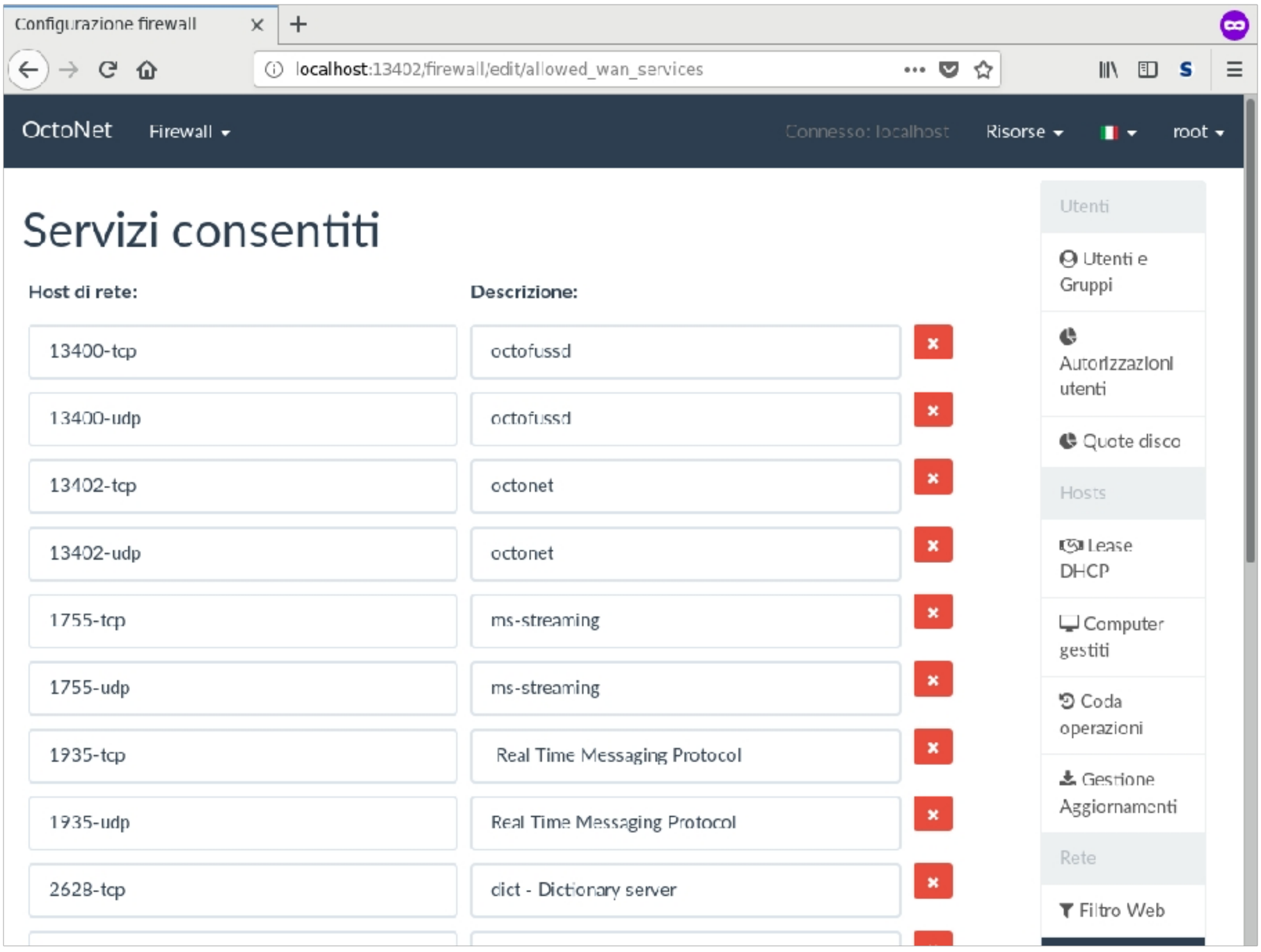
Host with full access corresponds to the file `/etc/fuss-server/firewall-allowed-lan-hosts`



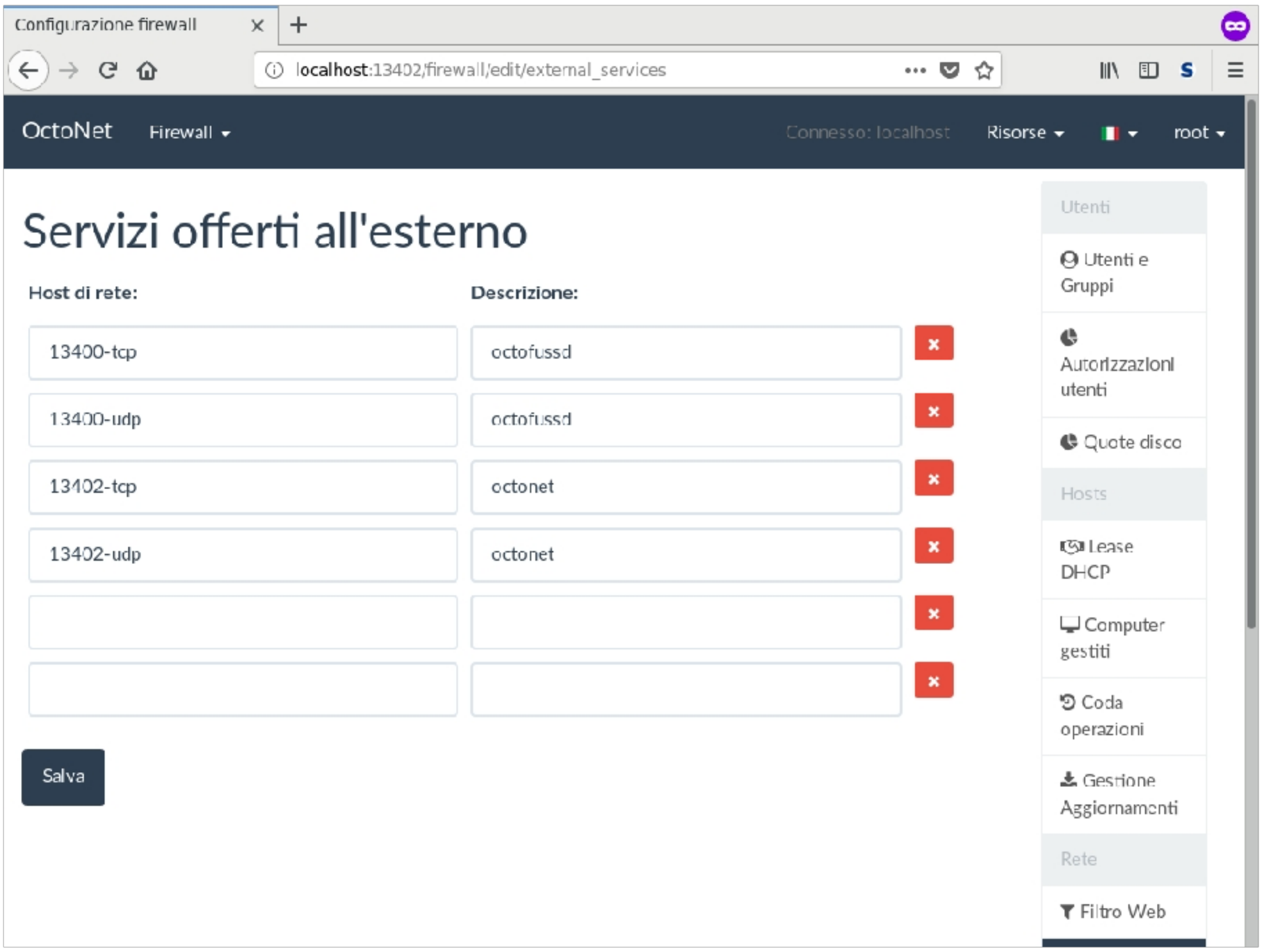
Allowed destinations corresponds to the file `/etc/fuss-server/firewall-allowed-wan-hosts`



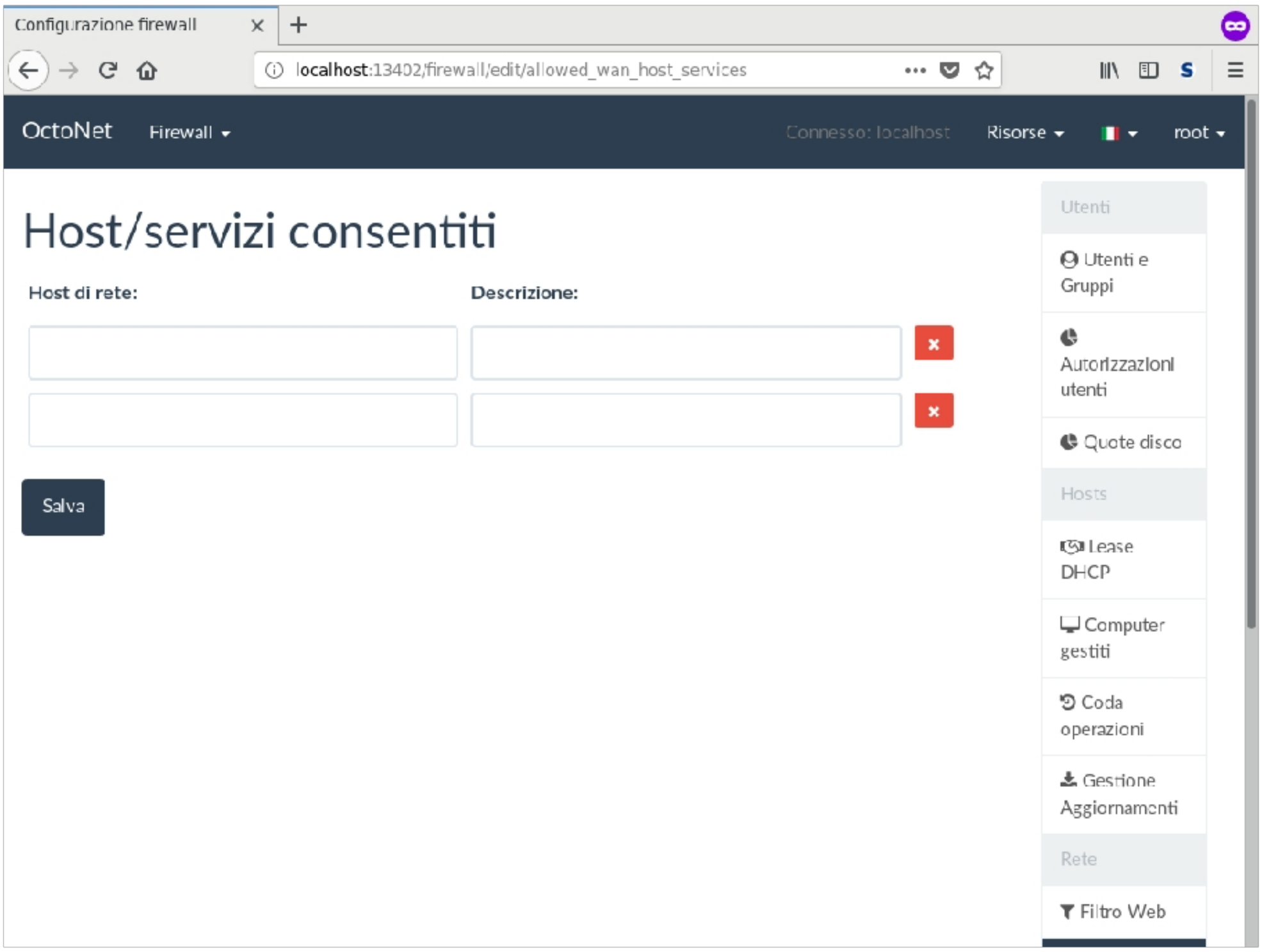
Allowed services corresponds to the file `/etc/fuss-server/firewall-allowed-wan-services`



Services offered externally corresponds to the file `/etc/fuss-server/firewall-external-services`



Allowed hosts/services corresponds to the file `/etc/fuss-server/firewall-allowed-wan-host-services`



5.5.1 Firewall changes

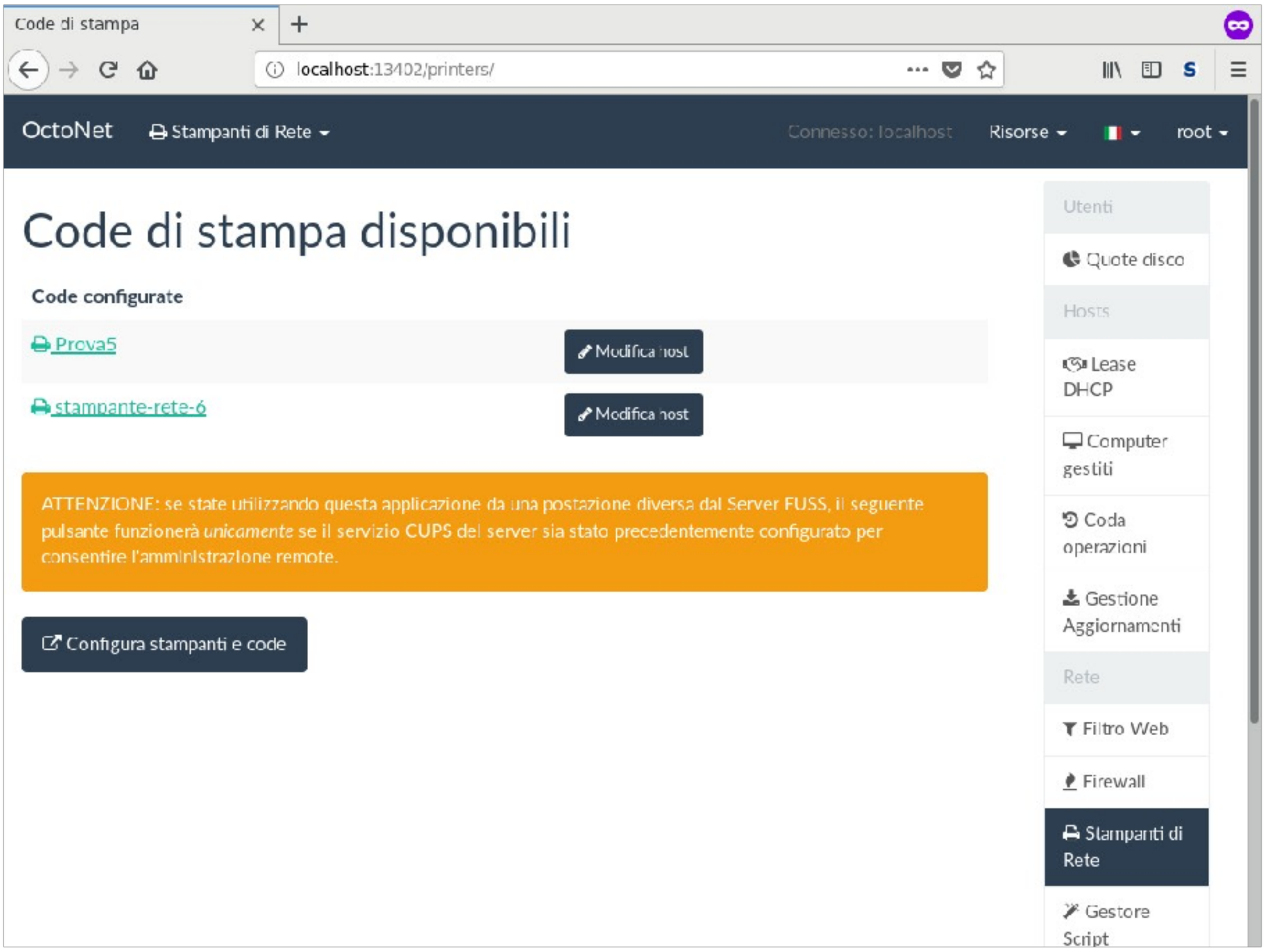
The fields on the pages just seen can be edited, or emptied by pressing the corresponding red x key; new entries can be added in the two blank lines at the bottom of the page.

For changes to be written to the configuration files, it is then necessary to press the *Save* button, and eventually restart the service from the main page of this section for them to become active.

5.6 Printers from network

The *Network → Network Printers* section allows you to manage shared printers.

The main page of the section presents the list of available printers (i.e., "print queues"), with links to the relevant configuration page, and a button that takes you to the configuration page of *CUPS*, the printer management service.



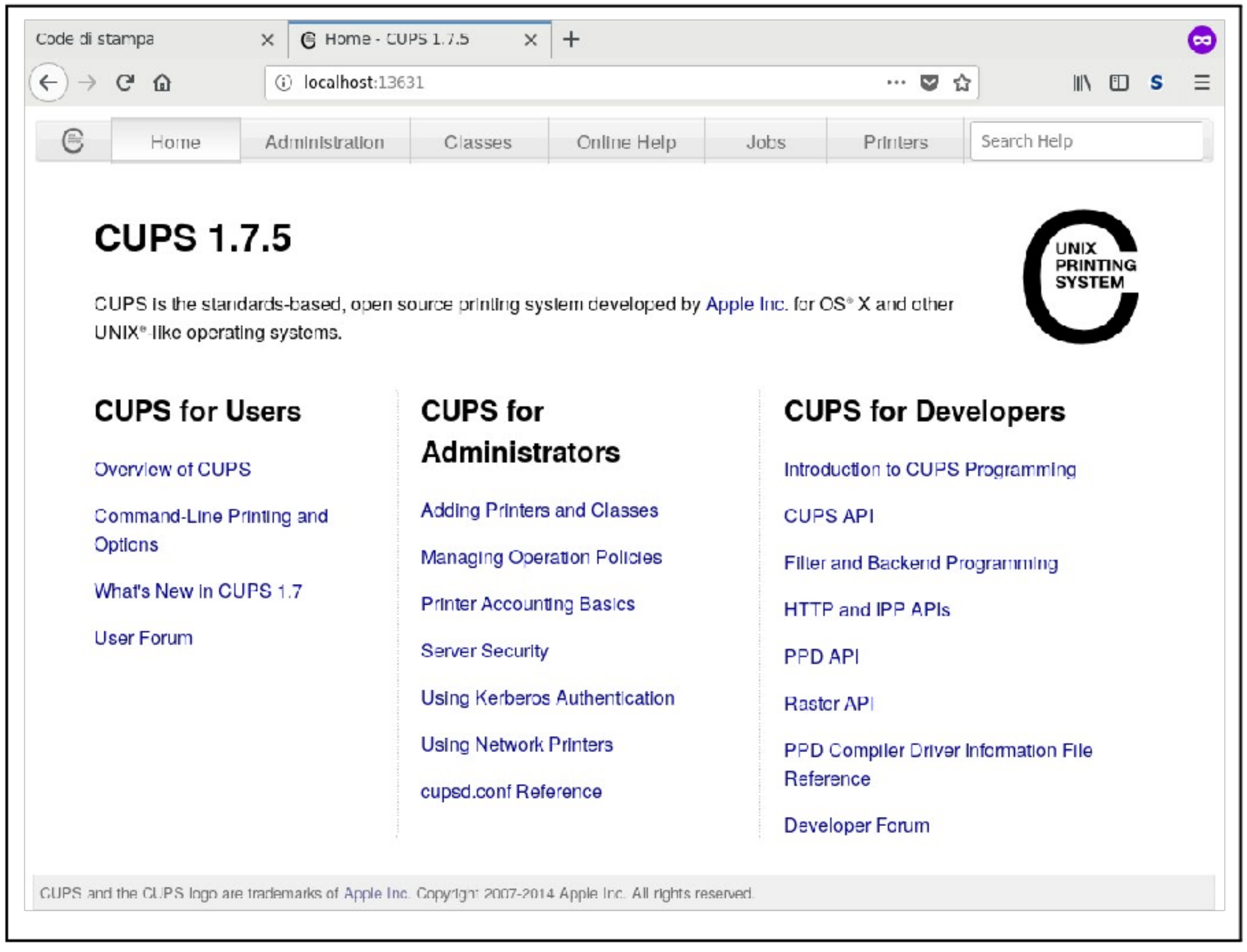
Access to CUPS is granted to root, or users in the `lpadmin` group.

Warning: If you are accessing OctoNet from a computer other than the server, via SSH tunnel, the *Configure Printers and Queues* link will point to the CUPS interface *of the machine you are accessing from* (if installed) and not the server.

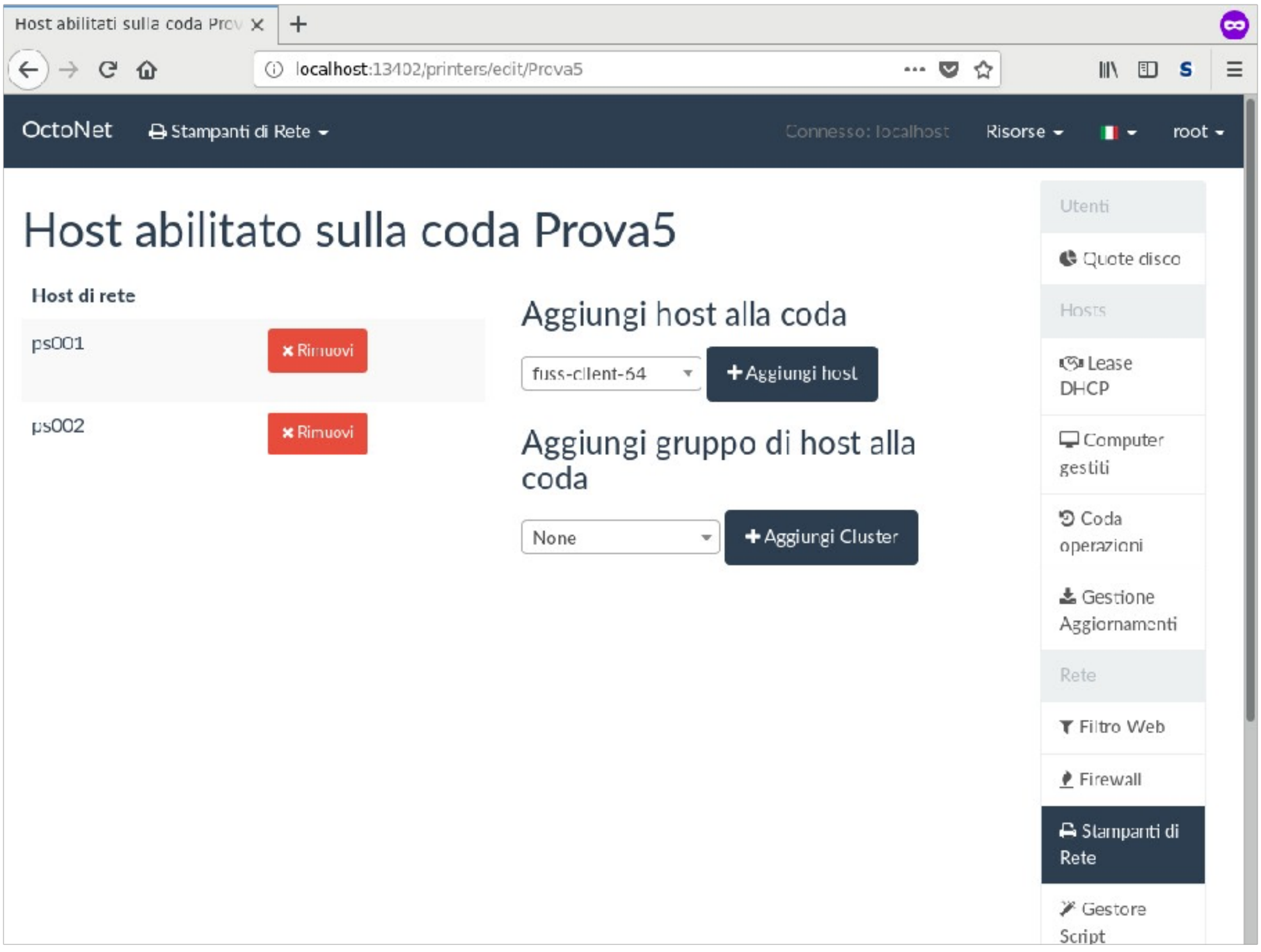
To access the CUPS interface of the server, a second ssh tunnel can be created with the command:

```
ssh sshuser@proxy -L 13631:localhost:631
```

and after opening *Configure Printers and Queues* manually correct the address because it points to http://localhost:13631/

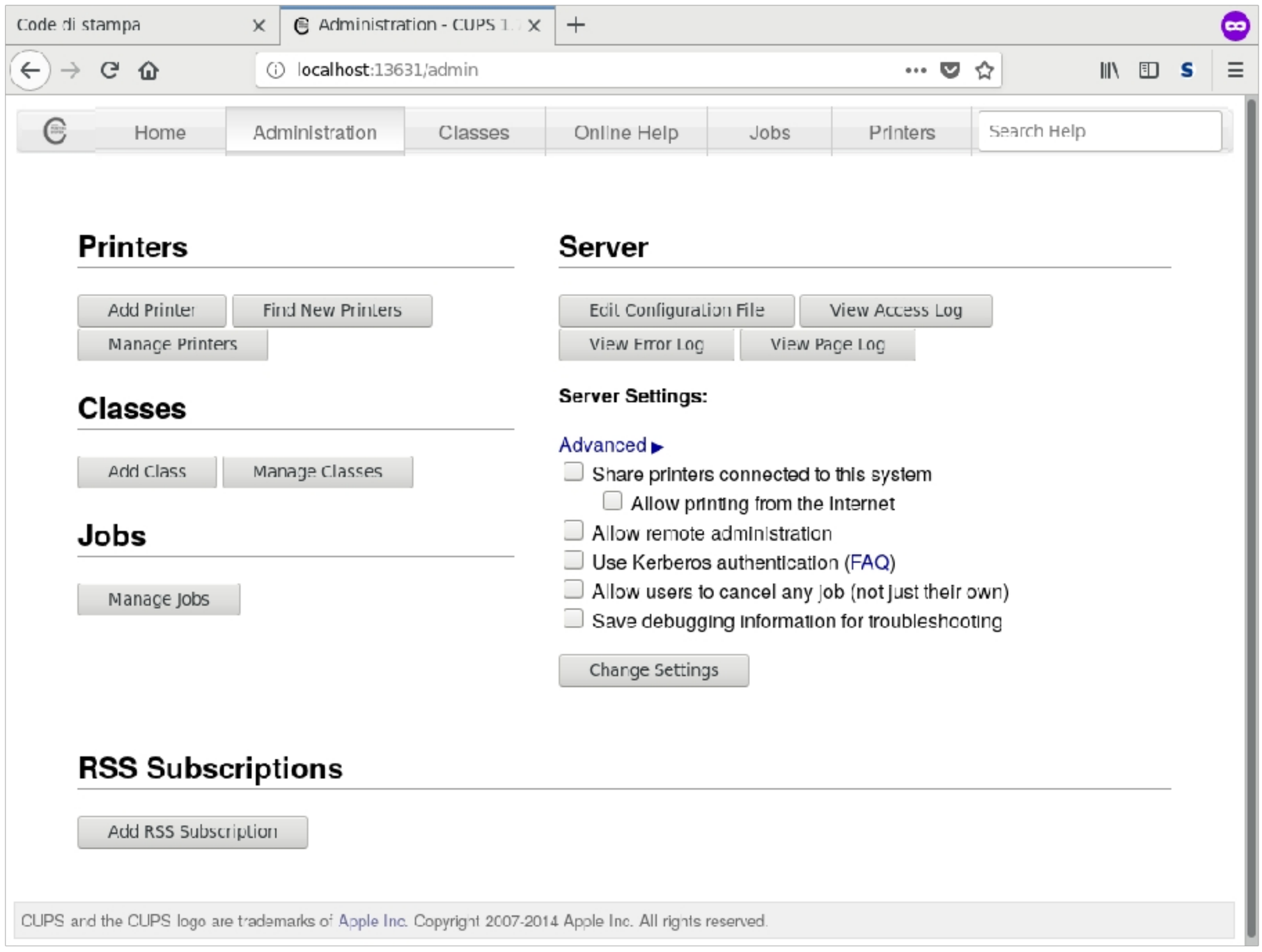


On the edit page of a print queue is a list of hosts on the local network enabled for access, with the ability to remove individual hosts from the list, add hosts (*Add Hosts to Queue*) or add with one click only all hosts that are part of a cluster (*Add Host Group to Queue*).



5.6.1 Adding a printer

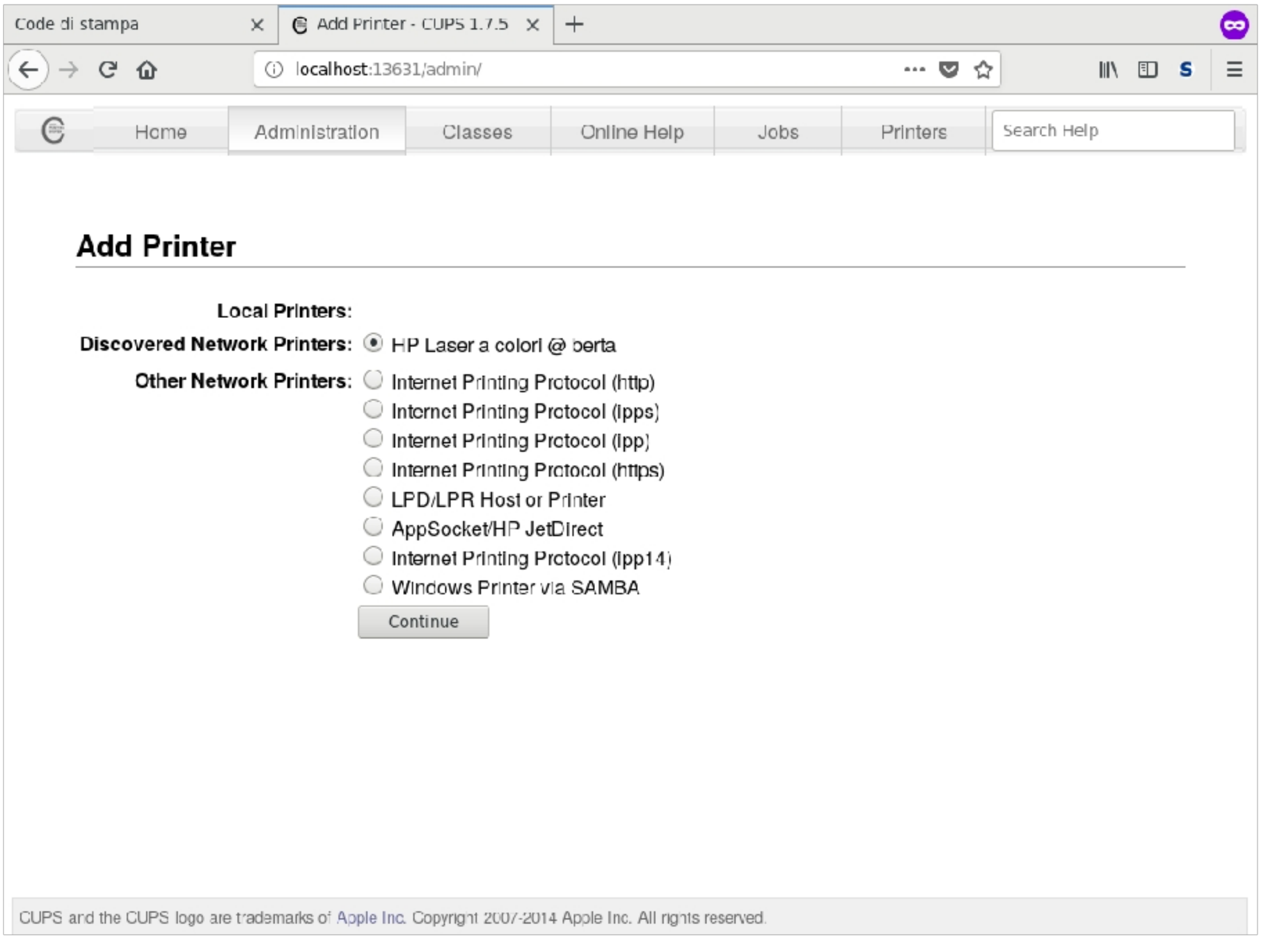
To add a new printer it is first necessary to configure it on CUPS: from the related interface select *CUPS for Administrators → Adding Printers and Classes*:



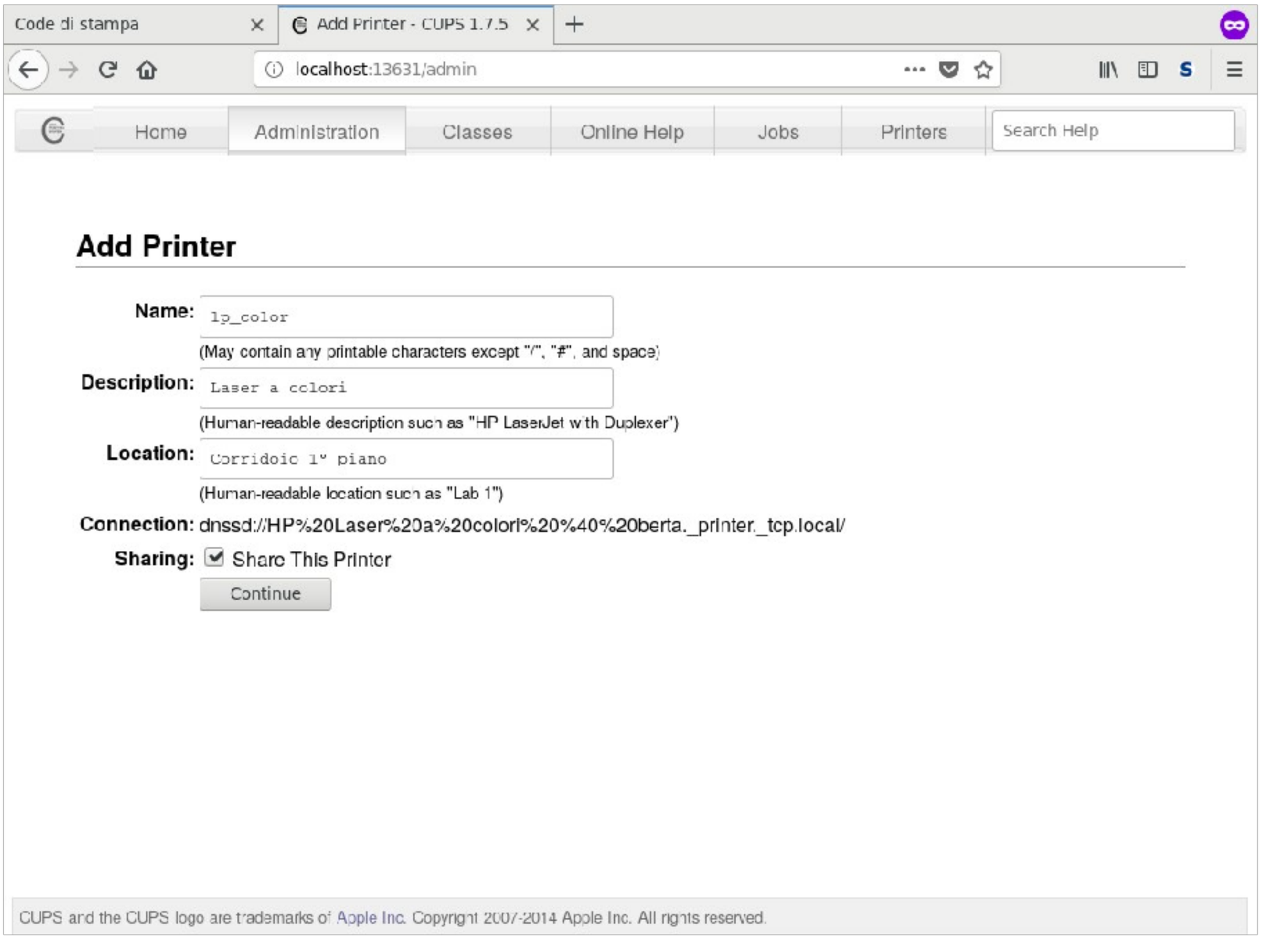
Then press the *Add Printer* button in the *Printers* section, authenticating with a user who is in the group `lpadmin` on the server.

Tip: Some printer models require additional steps for their installation in CUPS; for these see the *Managing and Installing Printers and Scanners* mini-guide.

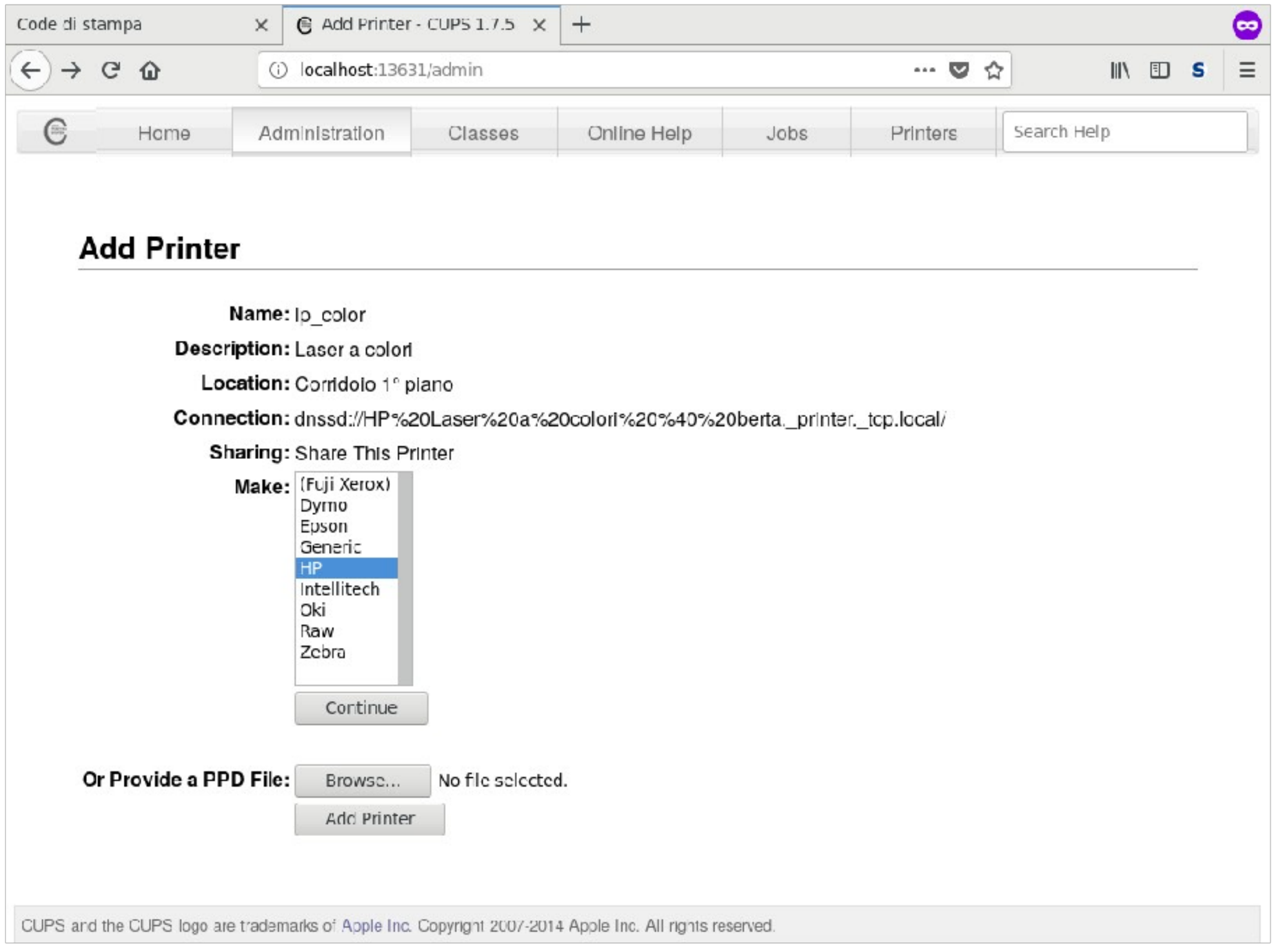
You will get a page with the choice of what type of printer to add; if local or network printers have already been found these will be presented in *Local Printers* or *Discovered Network Printers* respectively:



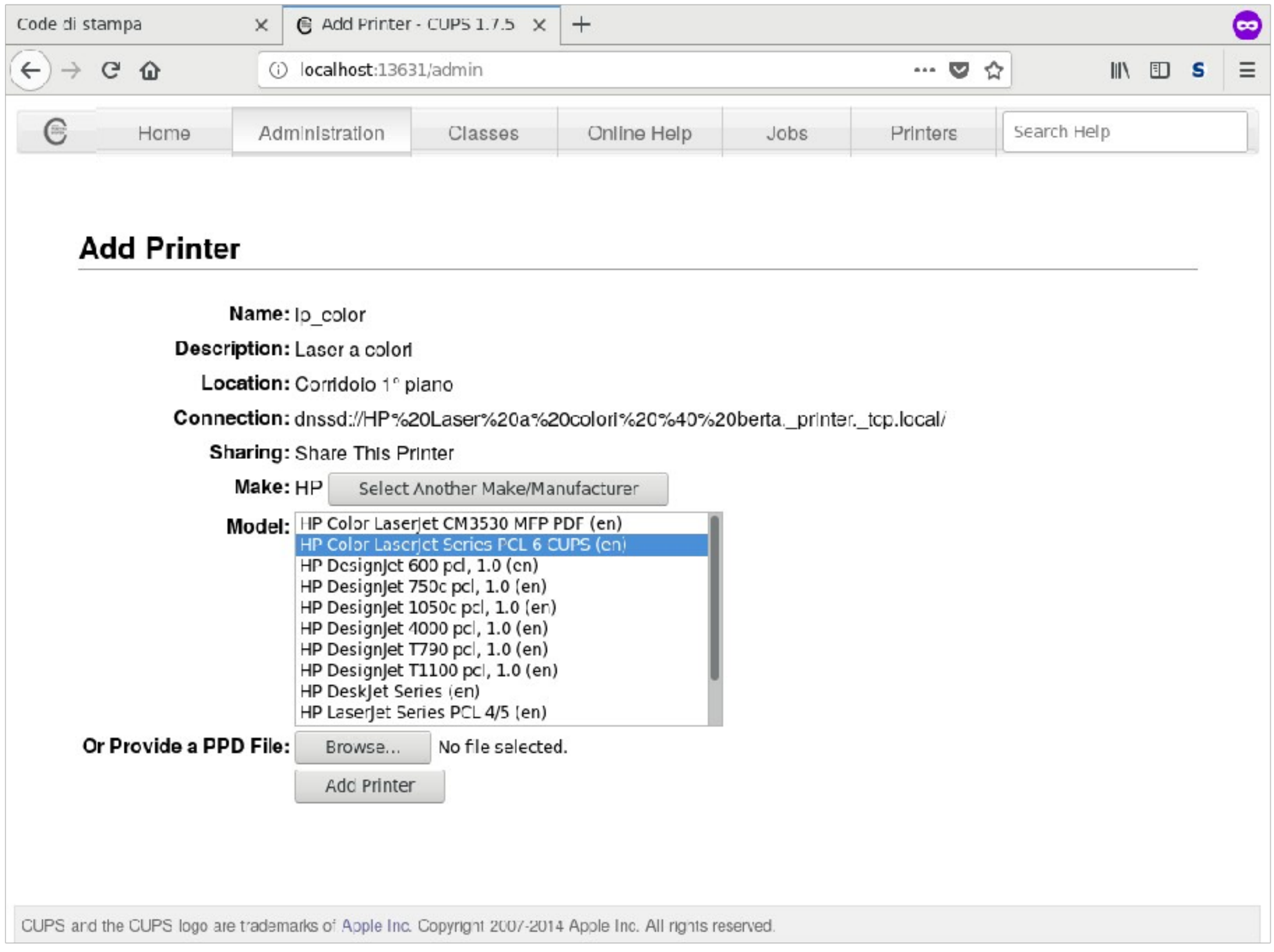
Selecting a printer that has already been recognized will prompt for a name (which cannot contain the characters `/`, `#` or space), a description, and a physical location to be displayed to users; it will also prompt whether to share the printer (*Share This Printer*):



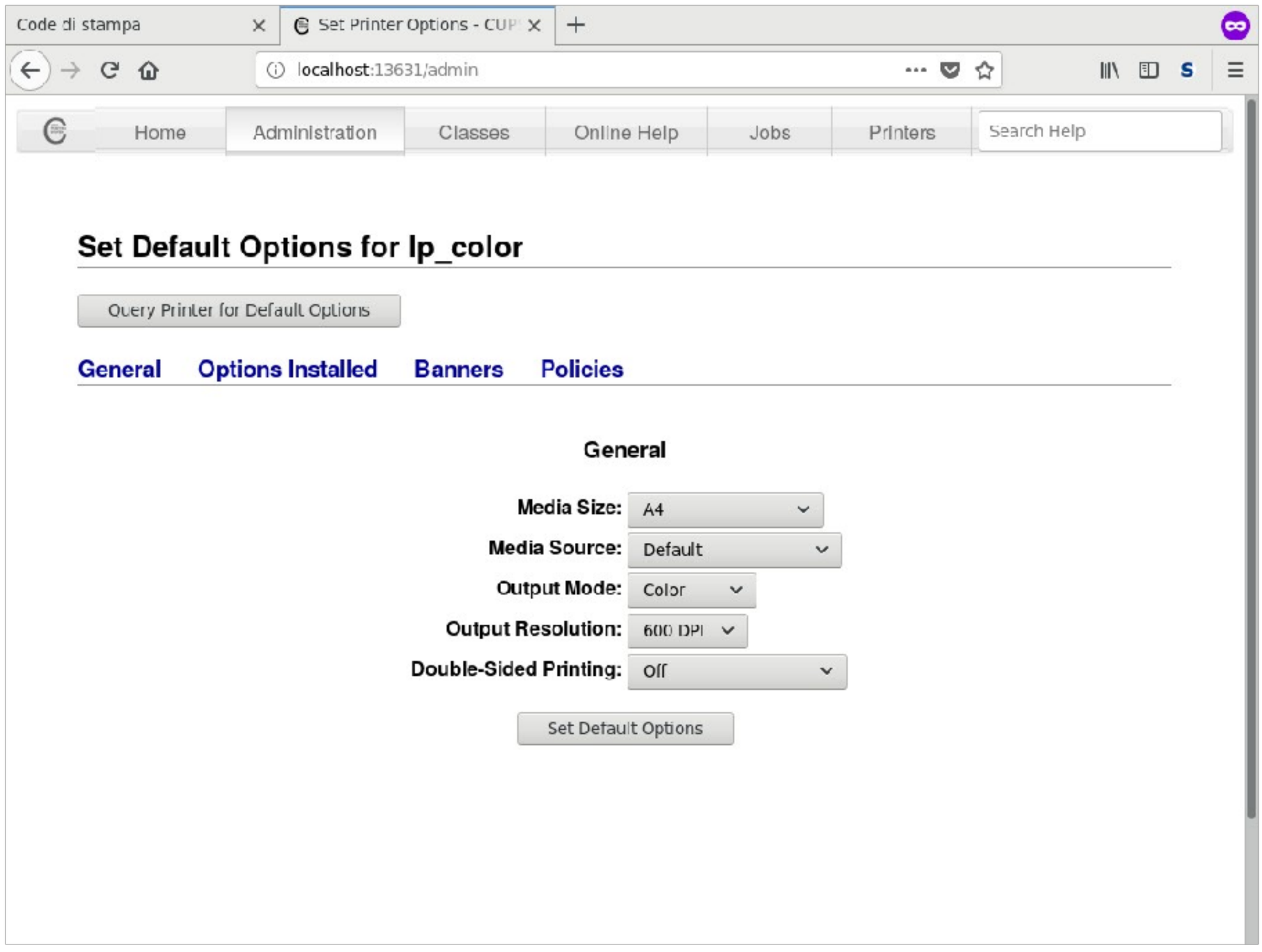
Pressing *Continue takes* you to the next screen, where you select the driver to be used for the printer by first indicating the manufacturer:



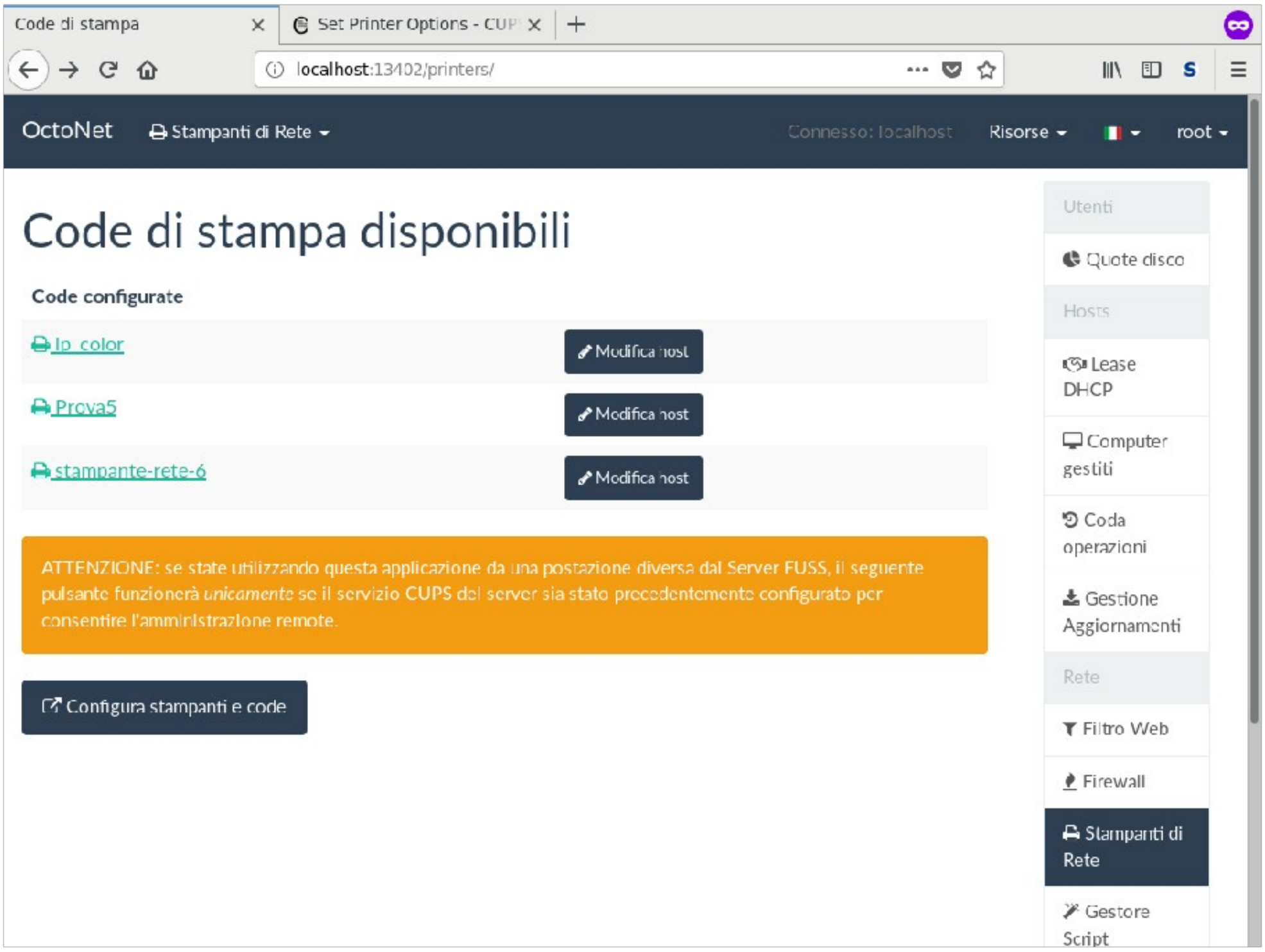
and, after pressing *Continue* the model:



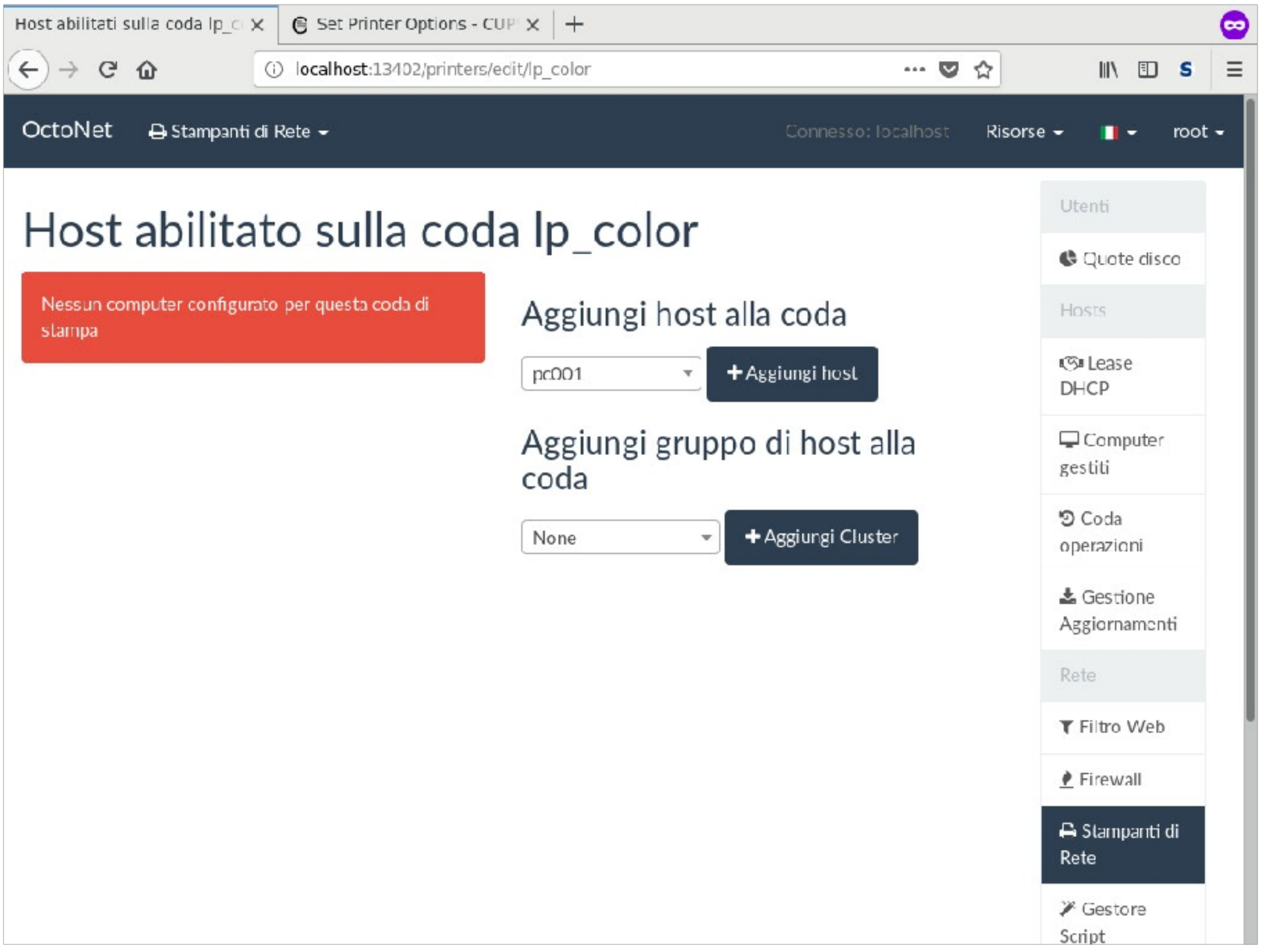
Pressing *Add* Printer adds the printer and takes you to a page where you can change its default settings:



At this point you can reload the octonet network printers page, where the printer you just added will have appeared:



And through *Edit Host* you can enable hosts to use it, thus completing the configuration of the new printer:



5.7 Share Samba

5.7.1 Creating a share

To create a samba share:

- Set up the directory on the filesystem, such as in a subdirectory of `/home/SAMBA`:

```
# mkdir /home/SAMBA/<share_name>.
```

  and assign appropriate permissions for users to access it; for example, to create a share writable by teachers:

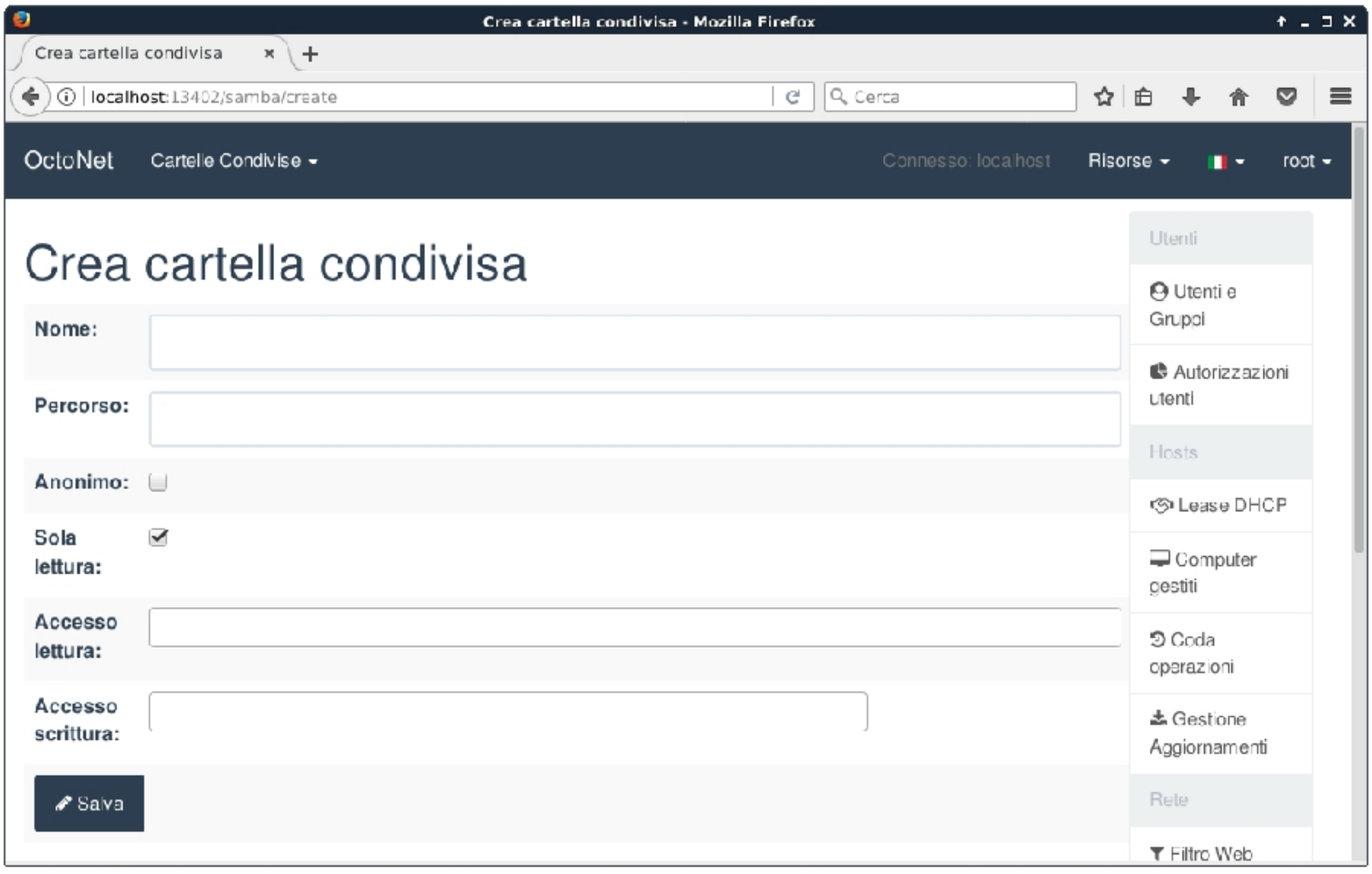
```
# chgrp faculty /home/SAMBA/<share_name>
# chmod 775 /home/SAMBA/<share_name>
```

- via octonet, go on creating a new share:
  - Shared Folders → Samba Service in the side menu;
  - Shared Folders → Create Shared Folder in the top menu; (page

  will open at `/samba/create`)
- indicate:
  - SHARE NAME
  - absolute path
  - Any access parameters (guest, user groups with read access, write access etc)

Warning: Samba share names should consist of lowercase letters only to avoid errors in later use.

Newer versions of octonet prevent the inclusion of different characters in the share name.



5.7.2 Testing a share

Use any samba client to try shares.

From the command line

For example, with command-line `smbclient`, installed on a fuss-client, one can list the shares available on the server (and visible to the user in use) with:

```
$ smbclient -L proxy
```

And one can connect with:

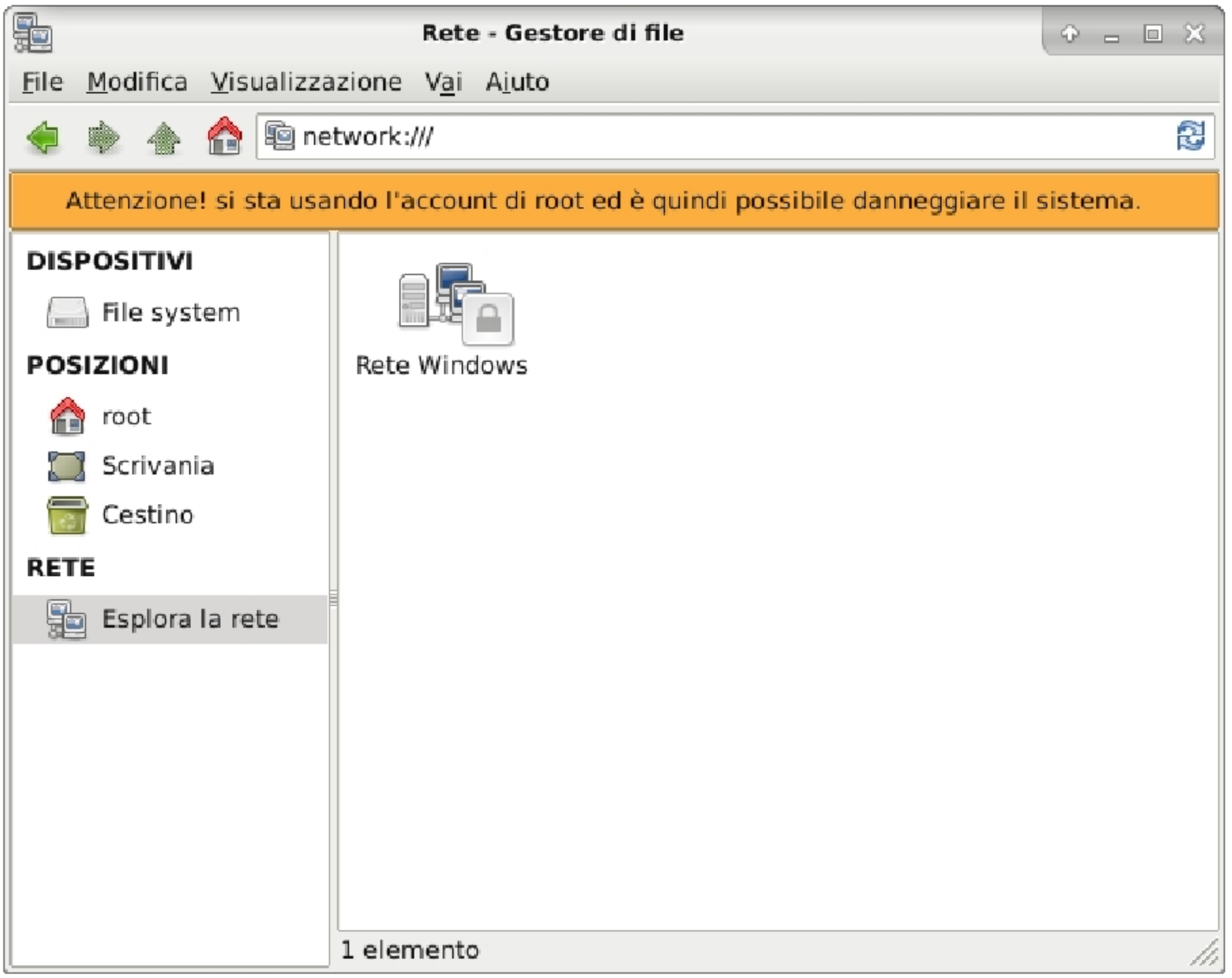
```
$ smbclient \\\\proxy\<share name>
```

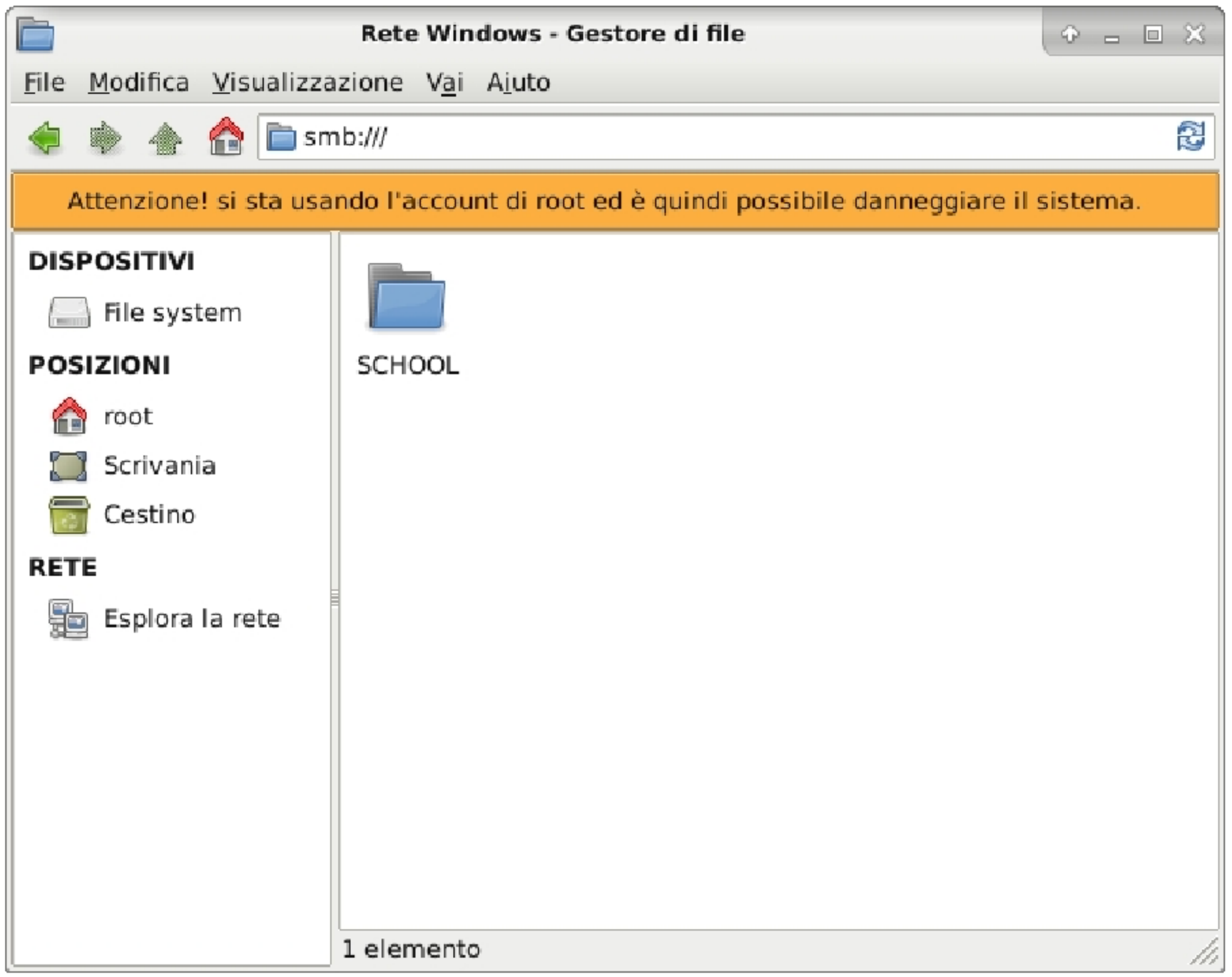
use `ls` to see the files present, quit to exit, `help` to see the other available commands.

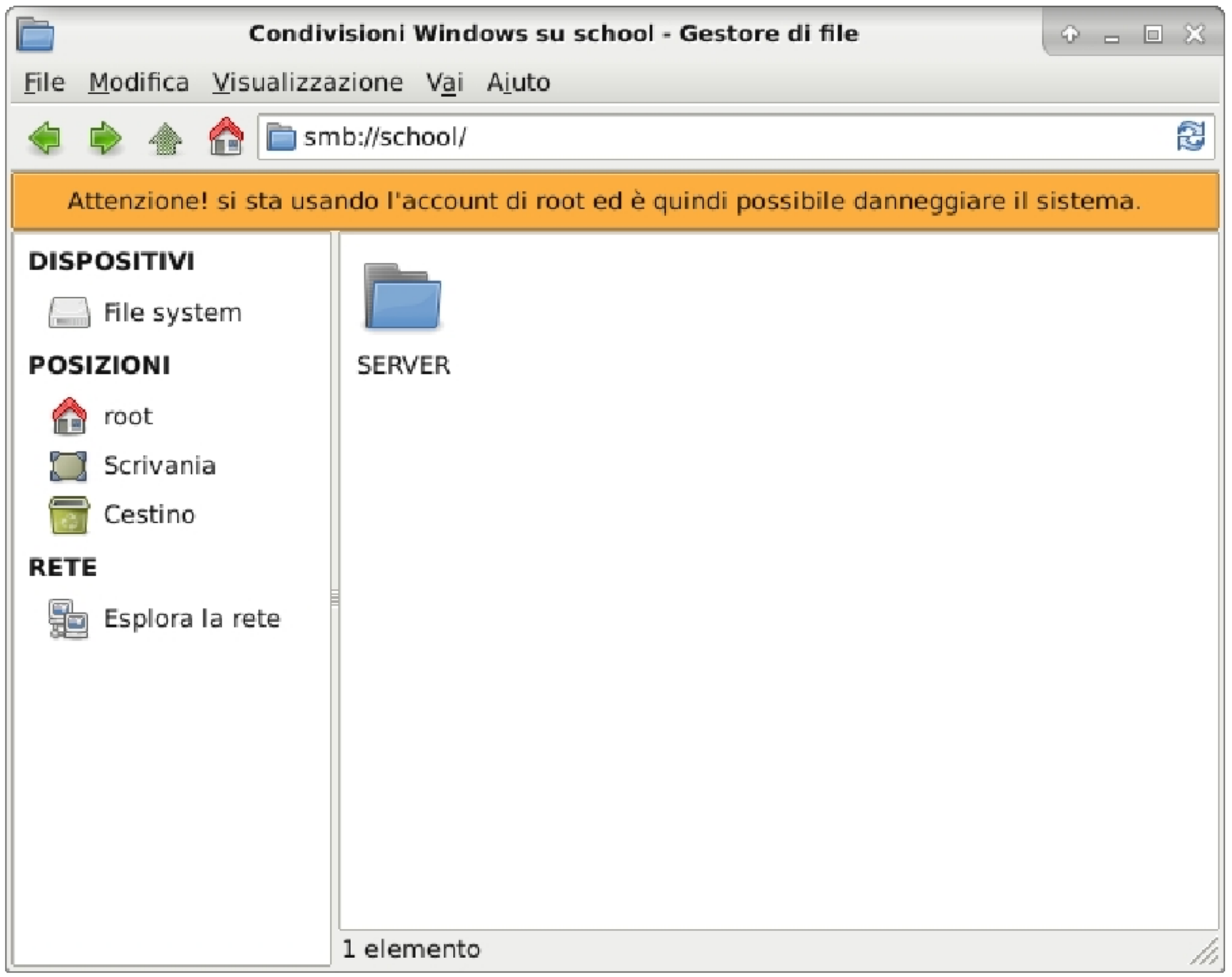
With Thunar (Graphical File Manager)

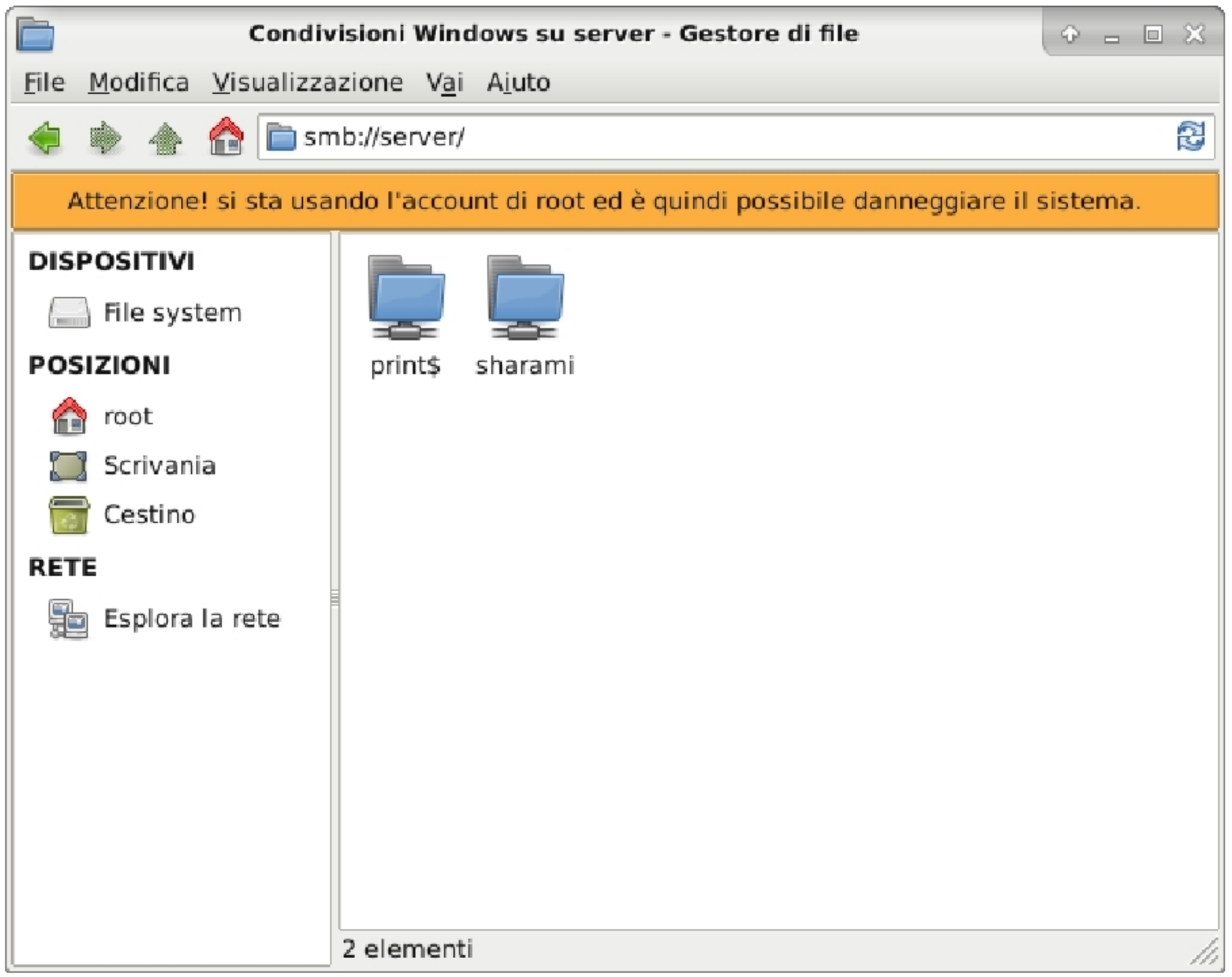
The fuss-client File Manager is capable of accessing samba shares; you can then use it to test its configuration.

In the side column, select "Explore the Network," then open "Windows Network" and subsequent folders until you get to the desired share.


Rete - Gestore di file
File Modifica Visualizzazione Vai Aiuto
network:///
Attenzione! si sta usando l'account di root ed è quindi possibile danneggiare il sistema.
DISPOSITIVI
File system
POSIZIONI
root
Scrivania
Cestino
RETE
Esplora la rete
Rete Windows
1 elemento

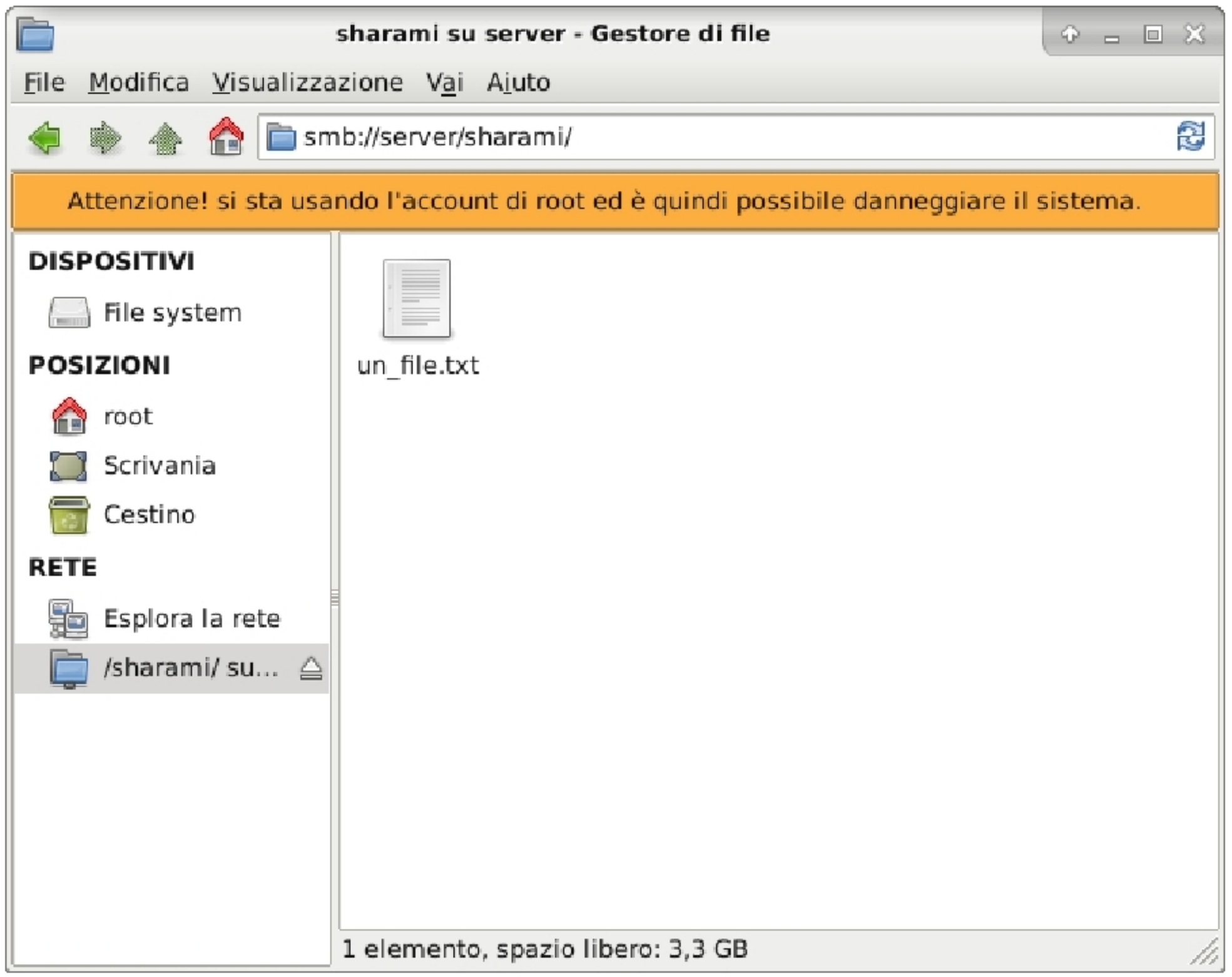

Rete Windows - Gestore di file
File Modifica Visualizzazione Vai Aiuto
smb:///
Attenzione! si sta usando l'account di root ed è quindi possibile danneggiare il sistema.
DISPOSITIVI
File system
POSIZIONI
root
Scrivania
Cestino
RETE
Esplora la rete
SCHOOL
1 elemento


Condivisioni Windows su school - Gestore di file
File Modifica Visualizzazione Vai Aiuto
smb://school/
Attenzione! si sta usando l'account di root ed è quindi possibile danneggiare il sistema.
DISPOSITIVI
File system
POSIZIONI
root
Scrivania
Cestino
RETE
Esplora la rete
SERVER
1 elemento



Enter the password of an appropriate user to verify proper visibility of the share.


Richiesta password per la condivisione sharami su server
Connetti in modo anonimo
Connetti come utente:
Nome utente:
root
Dominio:
WORKGROUP
Password:
Dimenticare la password immediatamente
Ricordare la password fino al termine sessione
Ricordare per sempre
Annulla
Connetti


sharami su server - Gestore di file
File Modifica Visualizzazione Vai Aiuto
smb://server/sharami/
Attenzione! si sta usando l'account di root ed è quindi possibile danneggiare il sistema.
DISPOSITIVI
File system
POSIZIONI
root
Scrivania
Cestino
RETE
Esplora la rete
/sharami/ su...
un_file.txt
1 elemento, spazio libero: 3,3 GB

6.1 Foreword

For orderly home management, we recommend organizing the home tree by separating according to hierarchy:

- plexus or school order;
- teachers or pupils;
- class (only for pupils).

For example, the homes of teachers in a middle school may be in:

```
/home/media/doctors/
```

Instead, pupils in a primary class (say 2c) will be in, for example:

```
/home/primary/pupils/class-2c-ele
```

To facilitate class management, such as easily eliminating outgoing classes, it is recommended to assign a corresponding **subgroup.** In the above case, the pupils would then belong to group 2c-ele. Of course, different class and group designations can be chosen, as long as they are consistent and homogeneous in the same plexus.

The execution of the script expects that, as desirable, all pupils in the same plexus belong to the same **primary group**. Otherwise, it will be necessary to adapt it to the specific situation or launch it, for example, for smaller groups.

6.1.1 Moving classes from one year to another

6.2 The script

The following year clearly the classes and groups will change (e.g. **class-2c-ele** will become **class-3c-ele** and the group **2c-ele** will become **3c-ele**.

The moving procedure is entrusted to a script and requires only special care in setting up the two csv files read by the script.

Obviously, it is recommended to analyze the script well to understand exactly what it performs. If in doubt, contact info@fuss.bz.it:

```
#! /bin/bash
# Let's first create a copy of ldap #
LDAP save
slapcat -l ldap-dump.ldif

### LDAP restore in case of problems
#systemctl stop slapd
#echo "Restoring LDAP"
#rm -rf /var/lib/ldap/*.
#slapadd < $BASE/ldap-dump.ldif
#chown openldap:openldap /var/lib/ldap/*
#systemctl start slapd

# Uncomment the following two lines and comment on the next one if
# you intend to proceed interactively

#echo "What is the primary group of users to be moved?"
#read_PRIMARY GROUP

#Replace to pupil-ele the primary group of pupils of the
#classes to be moved
GROUP_PRIMARY=pupils-ele
echo "Primary group: $GRUP_PRIMARY
GROUP" MEMBERS=`members -p
$GRUP_PRIMARY GROUP` echo "Members:
$MEMBERS"

# The following part of the script reads the csv file with the #
old and new class names. The output classes
# are moved to nonexistent classes (e.g., 4th grade, VI #
elementary or higher)
# A check is made to avoid a class
# overwrite the other one if the csv was processed badly, but you
risk # moving only part of the classes.
# In this case, it is preferable to restore the initial situation,
# fix the csv file and re-plan the script.


while IFS=, read -r OLDHOME NEWHOME
do
    if [ [ ! -d "$NEWHOME" ]
    then
        echo $NEWHOME
        mv $OLDHOME $NEWHOME
    else
        echo "Check the order of the classes in the csv!"
        exit
    fi
done < classes_mapping.csv

# With the following code, the same displacement of the
# classes in the ldap tree; in case of errors run the restore of #
ldap commented at the beginning of the script

declare -A classes; while IFS=, read -r OLDHOME NEWHOME ; do classes[$OLDHOME]=
↪$NEWHOME ; done < classes_mapping.csv

for i in `members -p $GRUPLE_PRIMARY`
do
    home=`smbldap-usershow $i |grep homeDirectory|awk '{print $2}'`
```

(continues on next page)

(continued from previous page)

```
    echo $home

    home_tr=${home/"/"$i/}

    echo $home_tr

    home_mod=${classes[$home_tr]}

    echo $home_mod

    smbldap-usermod -d $home_mod"/"$i $i

done

# Finally, if class_groups exist, with the following command you can
# update them from one year to the next by reading data from a csv.
# !!! Warning!!! To rename a group, it is necessary that the
# new group does not already exist, so the csv file should possibly
be # prepared with decreasing numbers from top to bottom!

while IFS=, read -r OLDGROUP NEWGROUP ; do smbldap-groupmod -n $NEWGROUP $OLDGROUP;
↪done < group_mapping.csv
```

6.3 The files csv

Here is an example csv (**classes_mapping.csv**) for moving classes. As you can see, the csv consists of two columns separated by a comma:

- the left column contains the "old" classes and the right column contains the "new" classes;
- note that the classes are in descending order from bottom to top;
- special care is taken in preparing the csv:

```
/home/primary/pupils/class-5b-ele,/home/primary/pupils/class-6b-ele
/home/primary/pupils/class-5a-ele,/home/primary/pupils/class-6a-ele
/home/primary/pupils/class-4b-ele,/home/primary/pupils/class-5b-ele
/home/primary/pupils/class-4a-ele,/home/primary/pupils/class-5a-ele
/home/primary/pupils/class-3b-ele,/home/primary/pupils/class-4b-ele
/home/primary/pupils/class-3a-ele,/home/primary/pupils/class-4a-ele
/home/primary/pupils/class-2b-ele,/home/primary/pupils/class-3b-ele
/home/primary/pupils/class-2a-ele,/home/primary/pupils/class-3a-ele
/home/primary/pupils/class-1b-ele,/home/primary/pupils/class-2b-ele
/home/primary/pupils/class-1a-ele,/home/primary/pupils/class-2a-ele
```

The following file (**group_mapping.**csv) is an example csv for moving class pupils from one group to the next. It is read in the same way as the previous one. If the new group already exists, the move does not take place, so you should always proceed in descending order from top to bottom, making sure that the highest groups (in our case **class-6. . . .**) do not exist, and delete them if necessary.

```
5b-ele,6b-ele
5a-ele,6a-ele
4b-ele,5b-ele
4a-ele,5a-ele
3b-ele,4b-ele
3a-ele,4a-ele
2b-ele,3b-ele
2a-ele,3a-ele
```

(continues on next page)

(continued from previous page)

```
1b-ele,2b-ele
1a-ele,2a-ele
```

6.4 Conclusions

The procedure described is necessary to keep the class layout in order as illustrated, but it can also be useful to heal untidy home trees or unclear names for pupils and teachers, such as **2019a** to denote **class-4th**. It all requires little time and only some care, we reiterate, in preparing the csv files.

CHAPTER 7

Fuss Manager

Fuss-manager is the new classroom management interface that will complement and gradually replace octonet.

This page will document its use.

CHAPTER 8

Specialized installations

We will discuss in this section a number of special cases for Fuss Server installation, not covered by the ordinary installation seen in the *traditional FUSS server installation* section

8.1 Installing Debian on RAID software

8.1.1 Preparing the machine

Sometimes it is possible that the server's RAID controller is not recognized in the installation (or that this is actually a fake raid) and therefore it is necessary to use the disks as singles without the BIOS RAID configuration. This for example is what happened with a Fujitsu PRIMERGY TX1320 M1 server with 2 hard drives of 1 Tb each in RAID1 (mirroring).

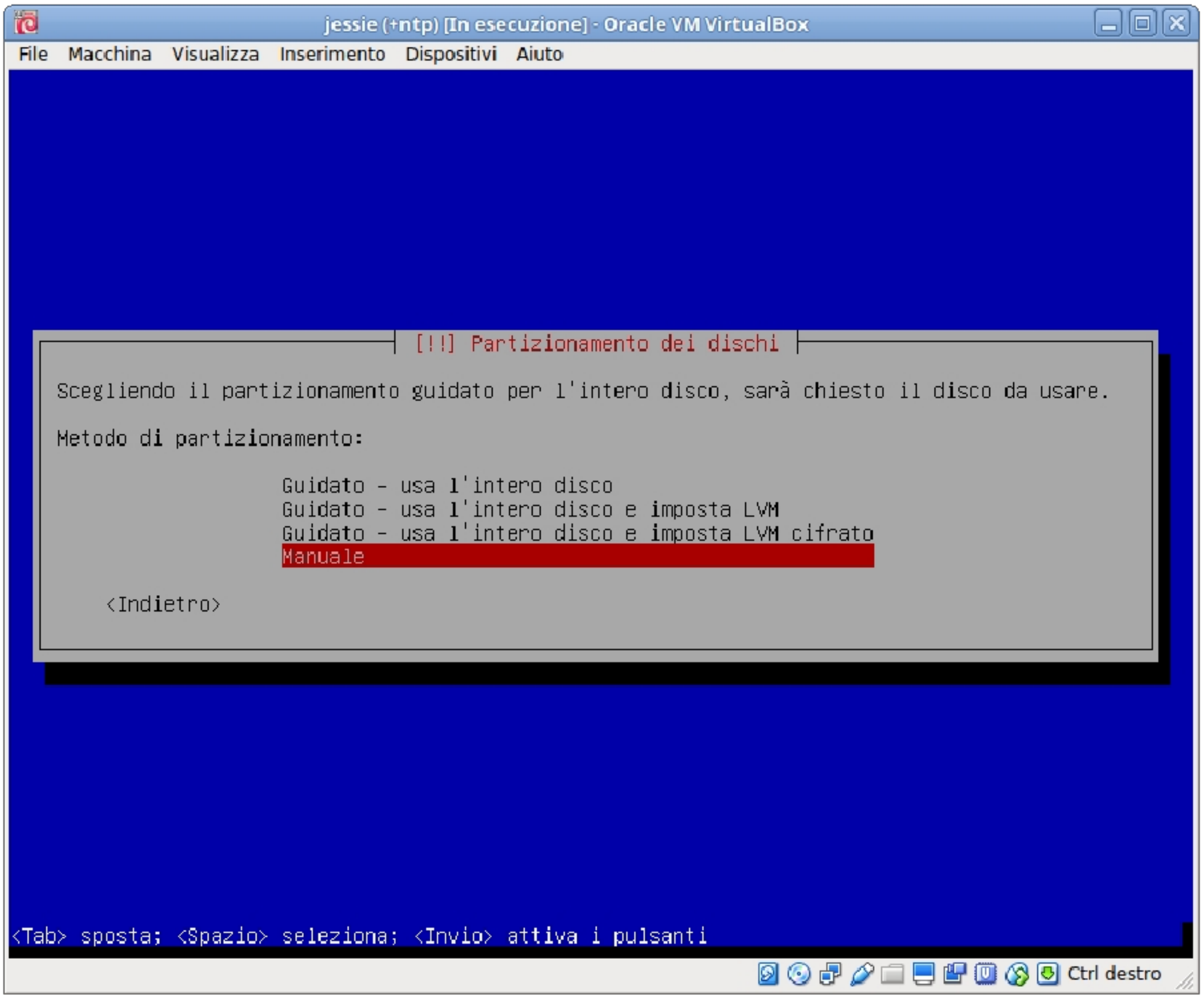
It is necessary in this case to make sure through the BIOS of the RAID controller that the HDs are simply in the "READY" state and possibly in the server BIOS (if possible) disable Controller_RAID.

Therefore, it is necessary, in the case of the Fujitsu PRIMERGY TX1320 M1, to enter the BIOS at startup with F2, after which from the BIOS perform the following steps:

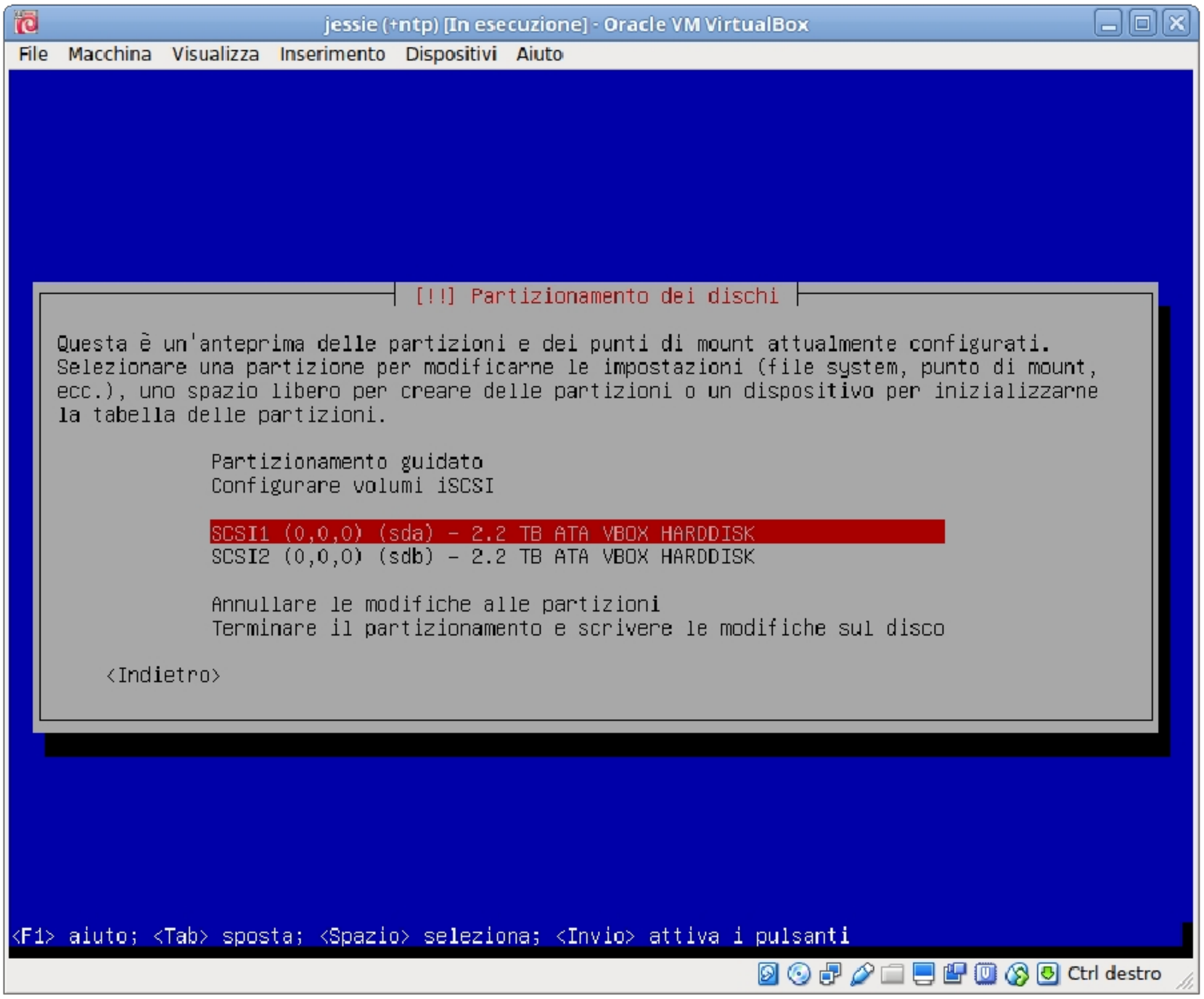
- Select Advanced
- Select SATA Configuration
- Select SATA Mode [AHCI MODE]
- Press F4 (Save and Exit) or select from menu "Save and Exit"

8.1.2 Disk partitioning

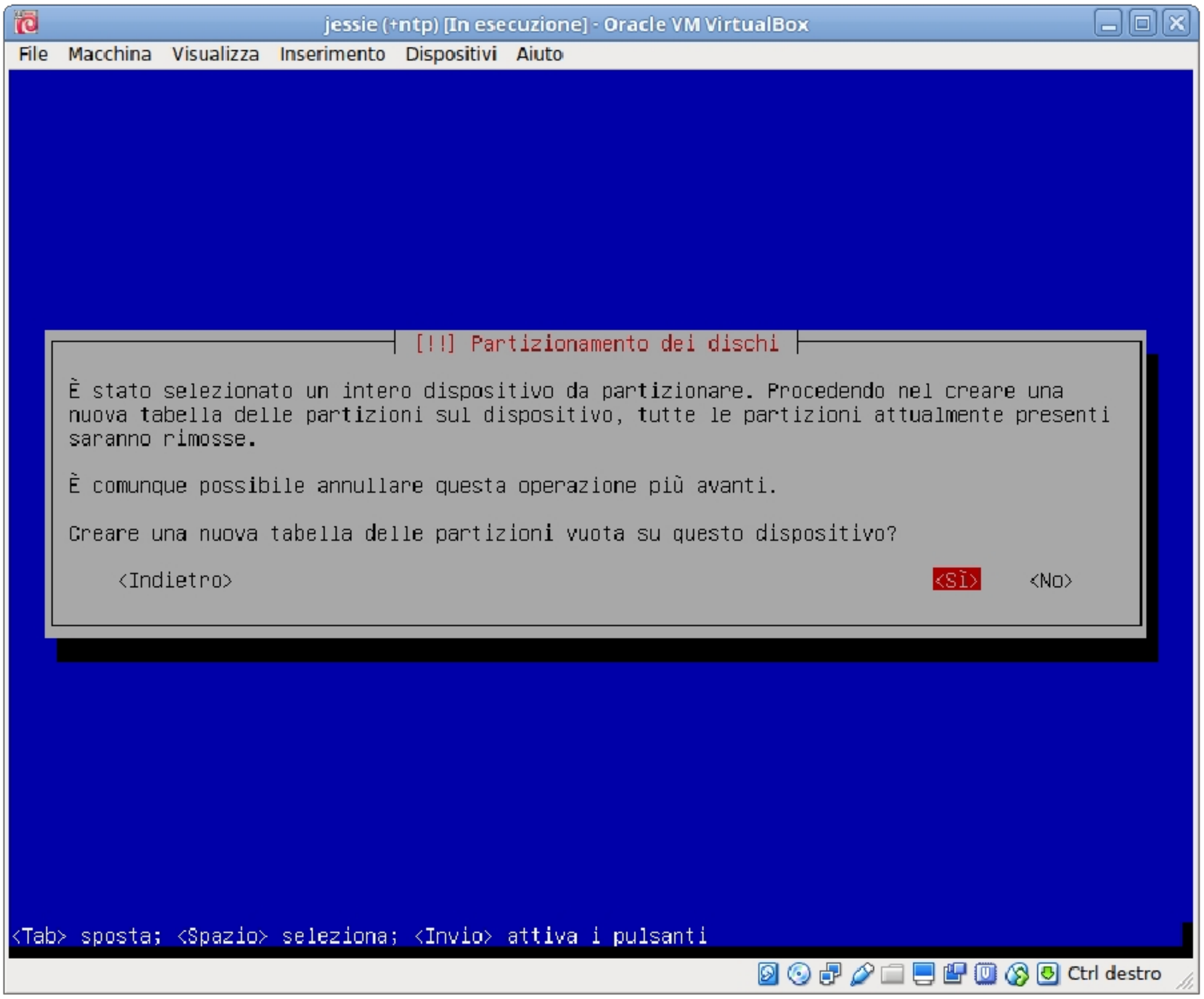
Once you have booted the machine with the Debian Buster installation CD/DVD/USB stick (take *the ul- test version available*) and arrived at the "Partitioning disks" screen, proceed by selecting
"Manual.



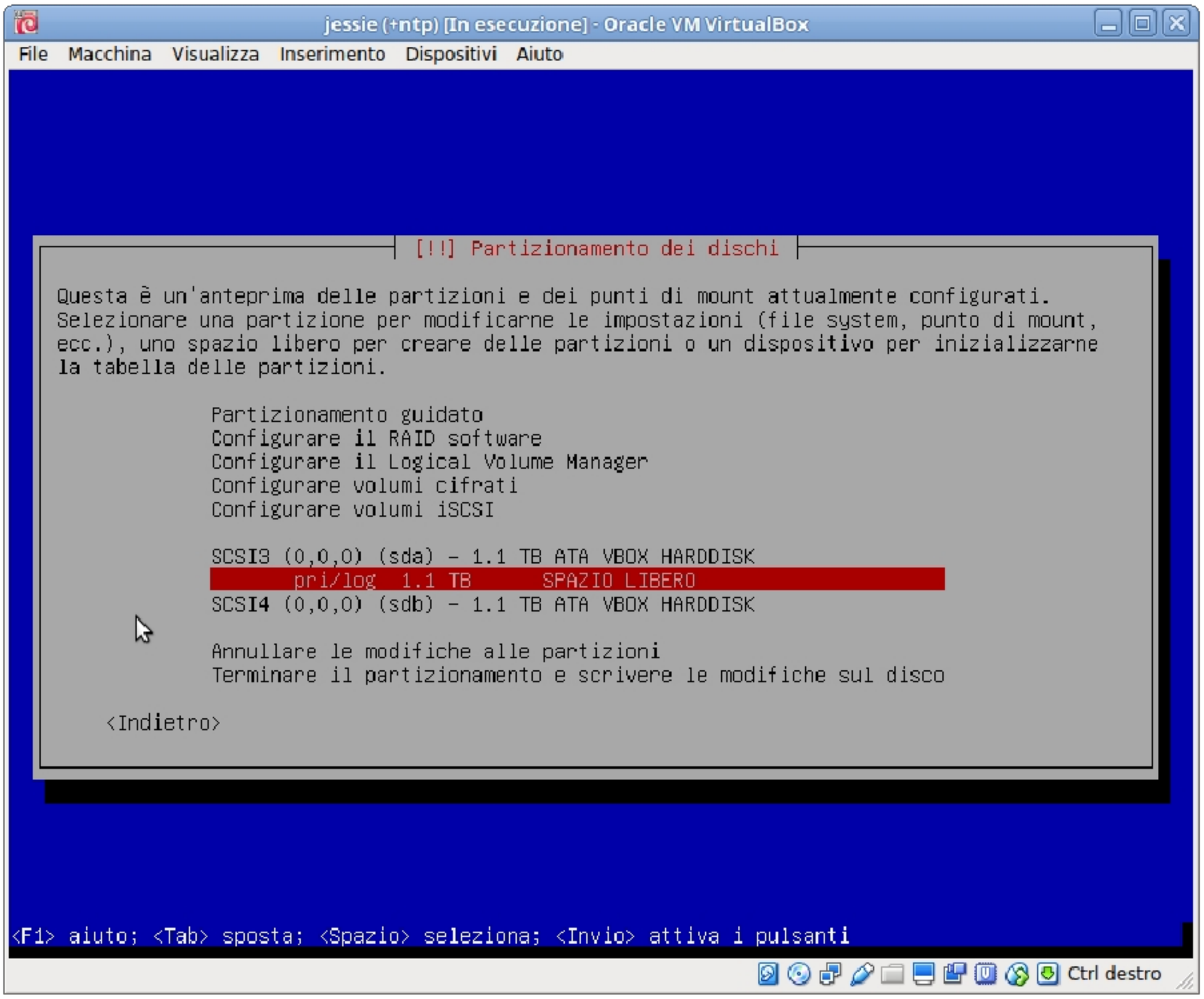
A list of disks (usually `sda` and `sdb`) will appear, and below each one, if any are present, that of any partitions.

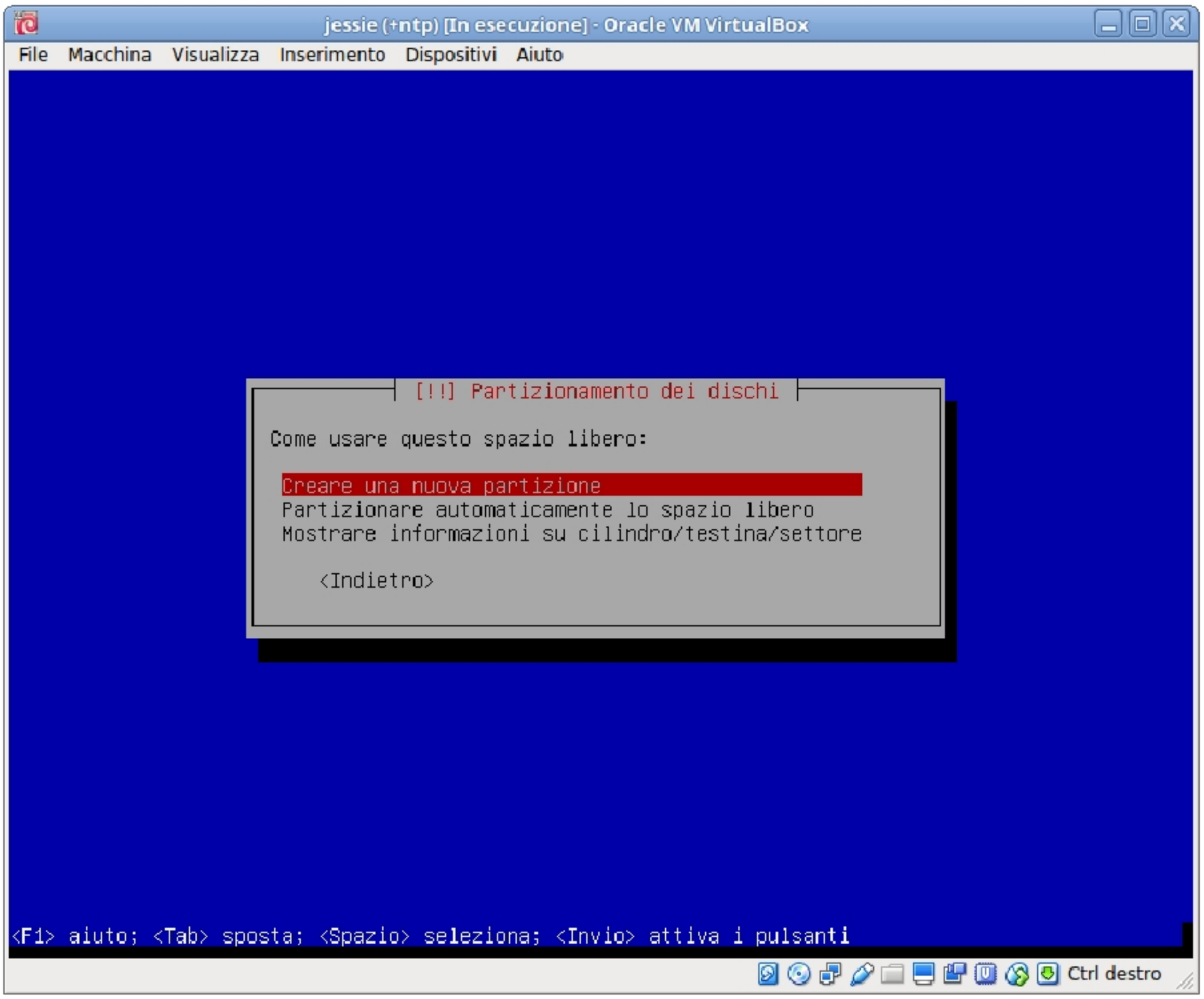


Whether partitions are present or not you will still need to position yourself on the line that lists the disk and select it with enter, which will lead to a prompt to create a new partition table, to which you must answer yes (if there are pre-existing partitions they will be deleted).

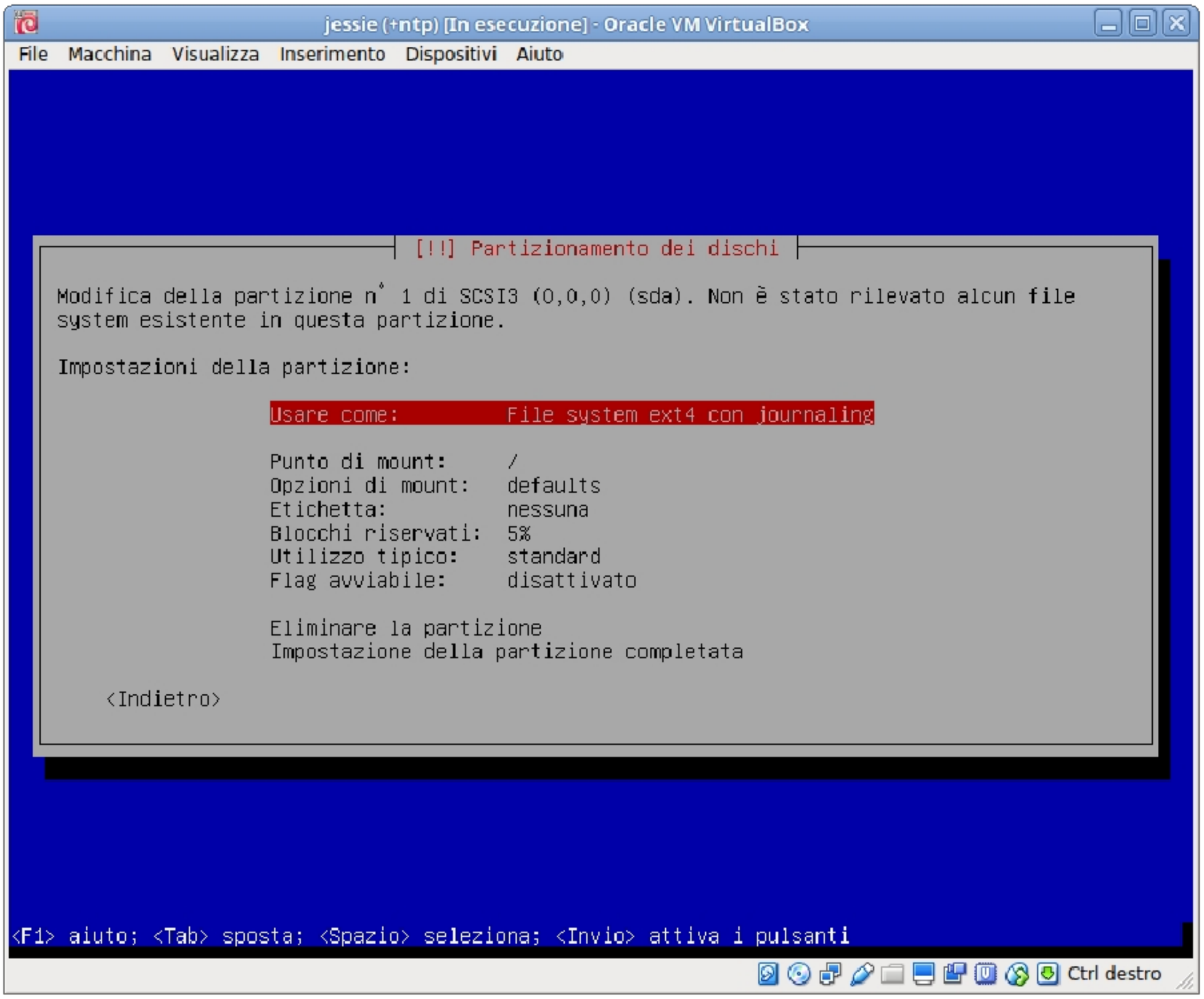


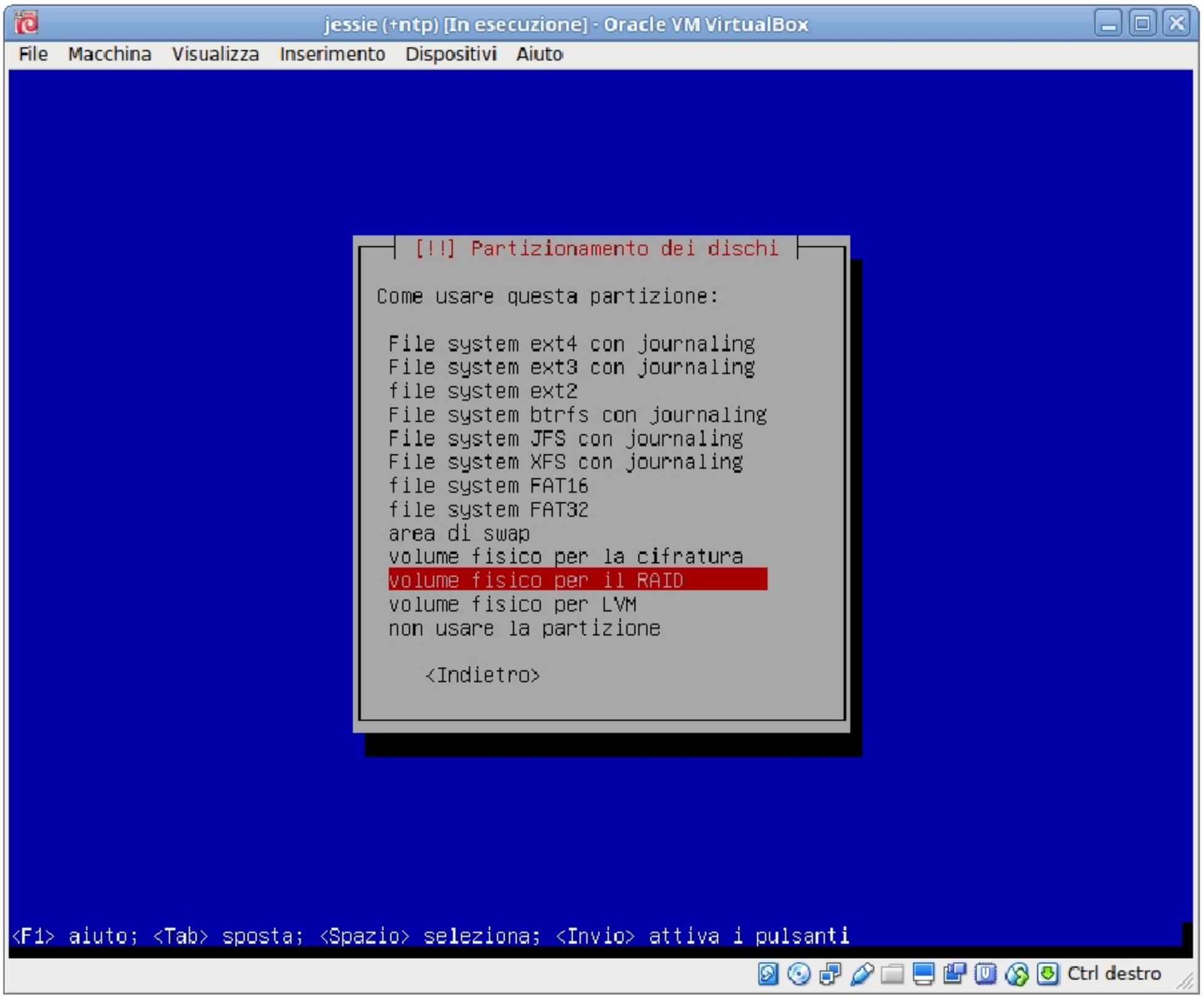
Now by selecting the "FREE SPACE" item that will appear below the disk you can proceed with partitioning by pressing enter, and choosing "Create a new partition."


jessie (+ntp) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
[!!] Partizionamento dei dischi
Questa è un'anteprima delle partizioni e dei punti di mount attualmente configurati.
Selezionare una partizione per modificarne le impostazioni (file system, punto di mount,
ecc.), uno spazio libero per creare delle partizioni o un dispositivo per inizializzarne
la tabella delle partizioni.
Partizionamento guidato
Configurare il RAID software
Configurare il Logical Volume Manager
Configurare volumi cifrati
Configurare volumi iSCSI
SCSI3 (0,0,0) (sda) - 1.1 TB ATA VBOX HARDDISK
pri/log 1.1 TB SPAZIO LIBERO
SCSI4 (0,0,0) (sdb) - 1.1 TB ATA VBOX HARDDISK
Annullare le modifiche alle partizioni
Terminare il partizionamento e scrivere le modifiche sul disco
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti
Ctrl destro

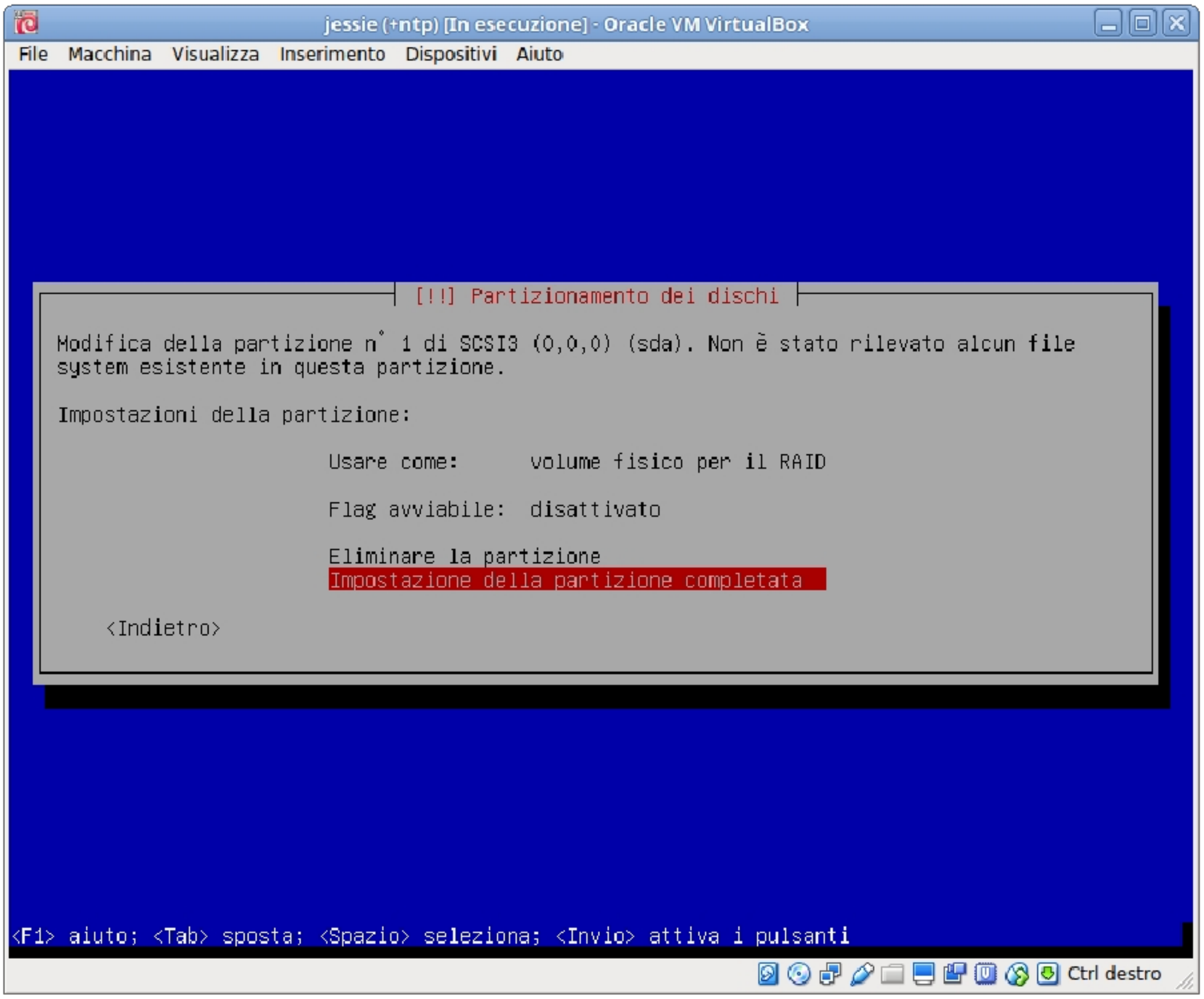


It will then be asked for its size. The first partition will be used to install RAID1 there, which will house `/boot` and its size can be between 512 Mb and 1Gb, so we will enter "1 Gb," for example, will then be asked for: the type of partition and "Primary" should be chosen, the location of the new partition and "Start" should be chosen, and finally the mode of use.


jessie (+ntp) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
[!!] Partizionamento dei dischi
Modifica della partizione n° 1 di SCSI3 (0,0,0) (sda). Non è stato rilevato alcun file system esistente in questa partizione.
Impostazioni della partizione:
Usare come: File system ext4 con journaling
Punto di mount: /
Opzioni di mount: defaults
Etichetta: nessuna
Blocchi riservati: 5%
Utilizzo tipico: standard
Flag avviabile: disattivato
Eliminare la partizione
Impostazione della partizione completata
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti
Ctrl destro

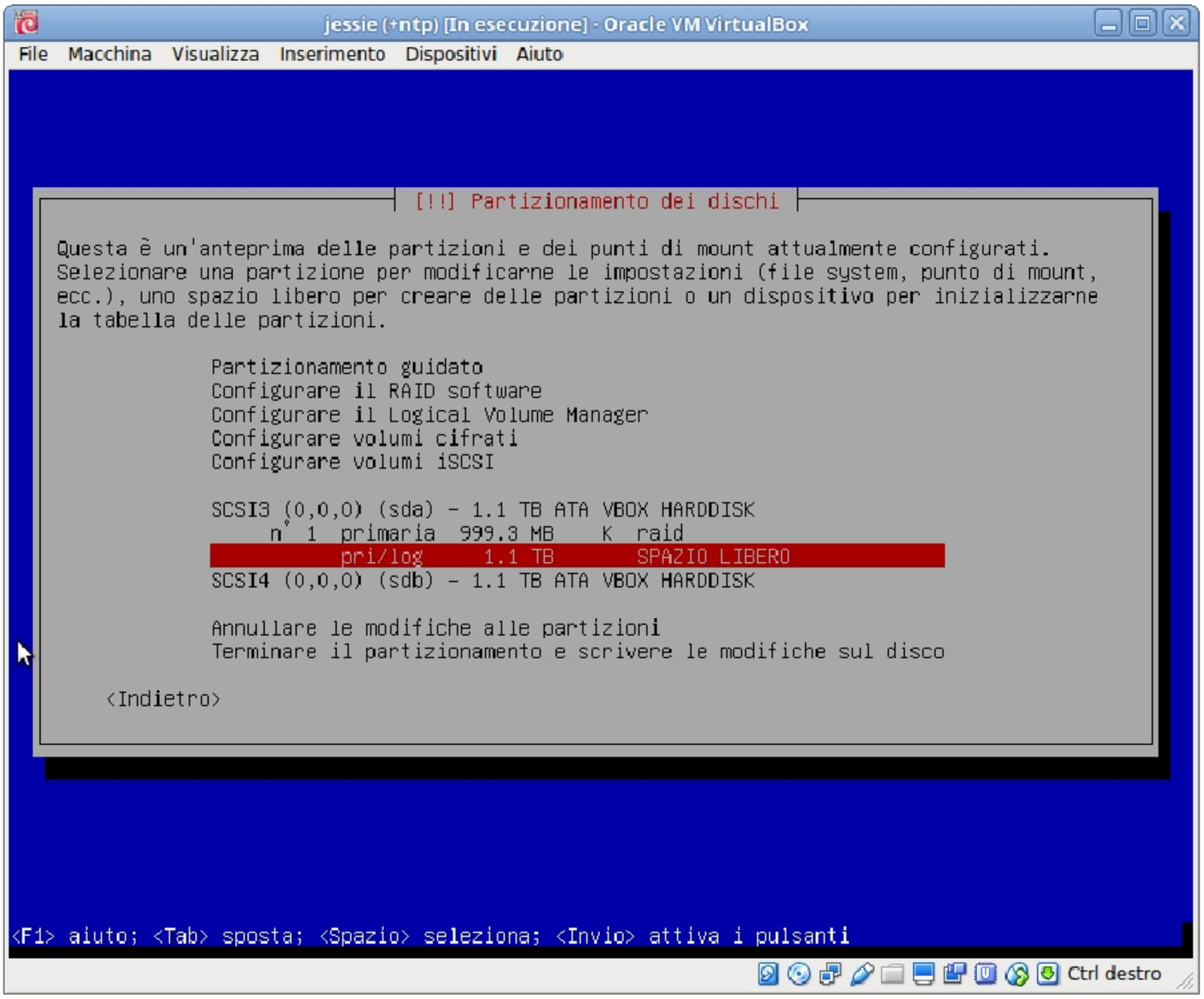


Here by pressing enter on the default value (usually "File system ext4 with Journaling") you need to select in the following me- nu "Physical volume for RAID," and having obtained the choice position yourself at the bottom of the screen on "Partition setting completed" and press enter.



The sequence for the first partition therefore is:

- Place on the disk (ex: `sda`)
- Create a new empty partition table on this device? <Yes>
- Stand on the free space
- Create a new partition
- 1 GB
- Primary;
- Beginning;
- Use as: Physical volume for RAID
- Partition settings completed



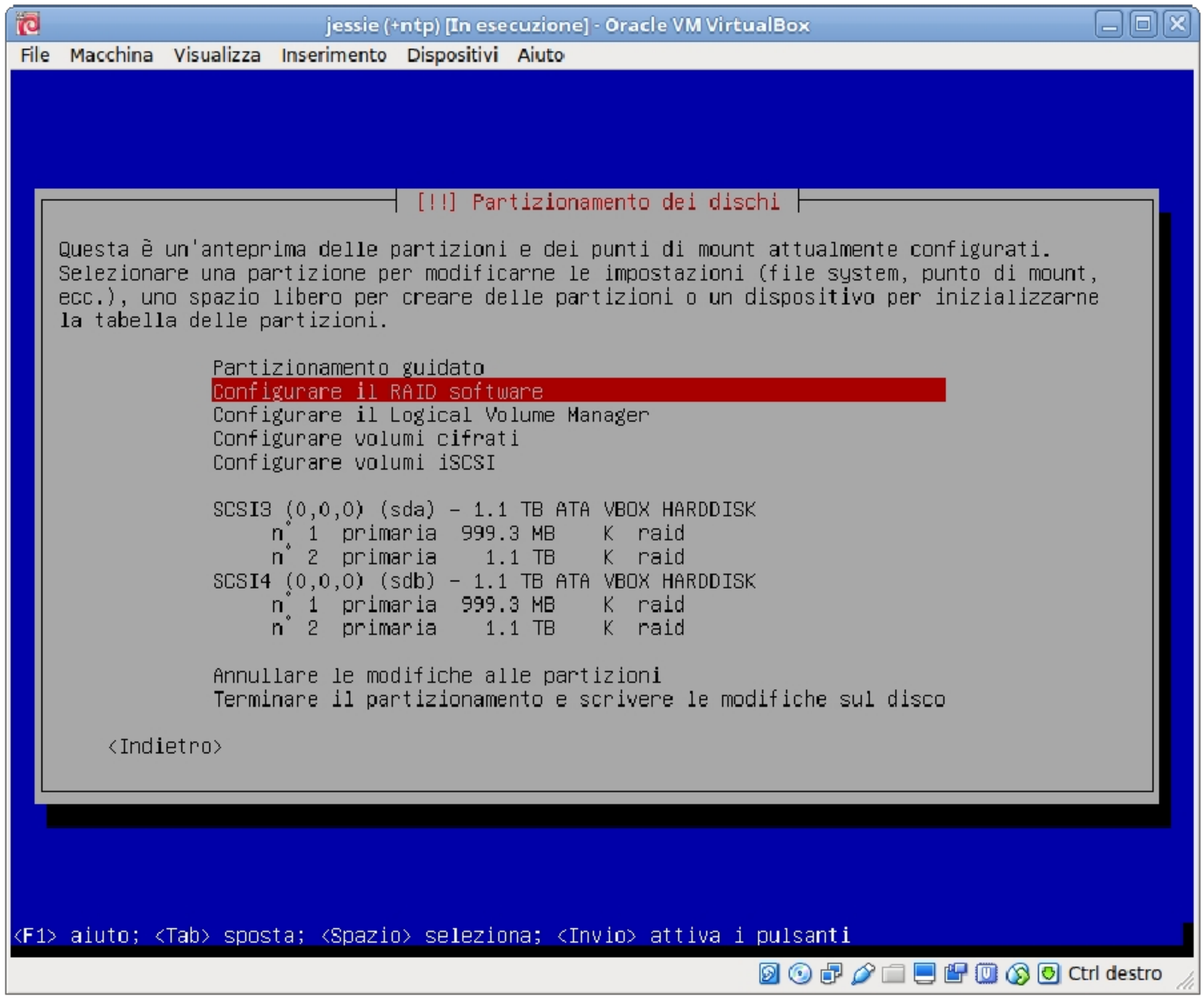
The operation should be repeated in a similar manner to create a second partition on the remaining free space, you will again have to select it on the next line, and repeat the same operations as the previous time accepting this time the proposed partition size (and reselecting the new partition as primary, as opposed to the default presented of logic), you will therefore have the sequence:

- Stand on the free space
- Create a new partition
- 999 GB (accept what is proposed)
- Primary;
- Beginning;
- Use as: Physical volume for RAID
- Partition settings completed

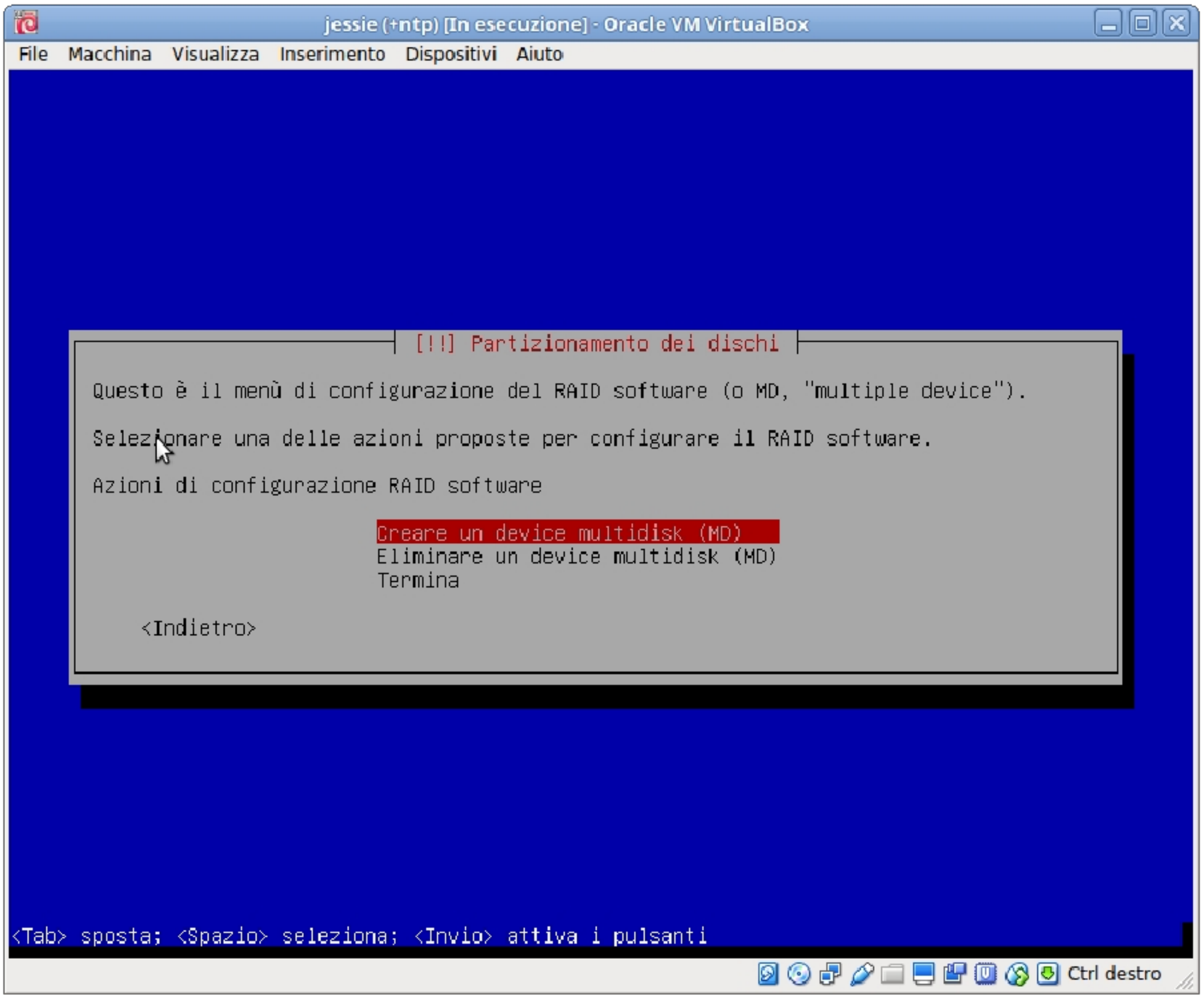
Once the partitioning of the first disk is completed, the operations will have to be repeated on the second disk (e.g. sdb), taking care to indicate exactly the same size: it is sufficient to indicate the same for the first partition, the second one with the default takes all the rest of the disk and will be the same in case of iden- tical disks (any small differences in case of different disks will leave the excess part of the larger one unused).

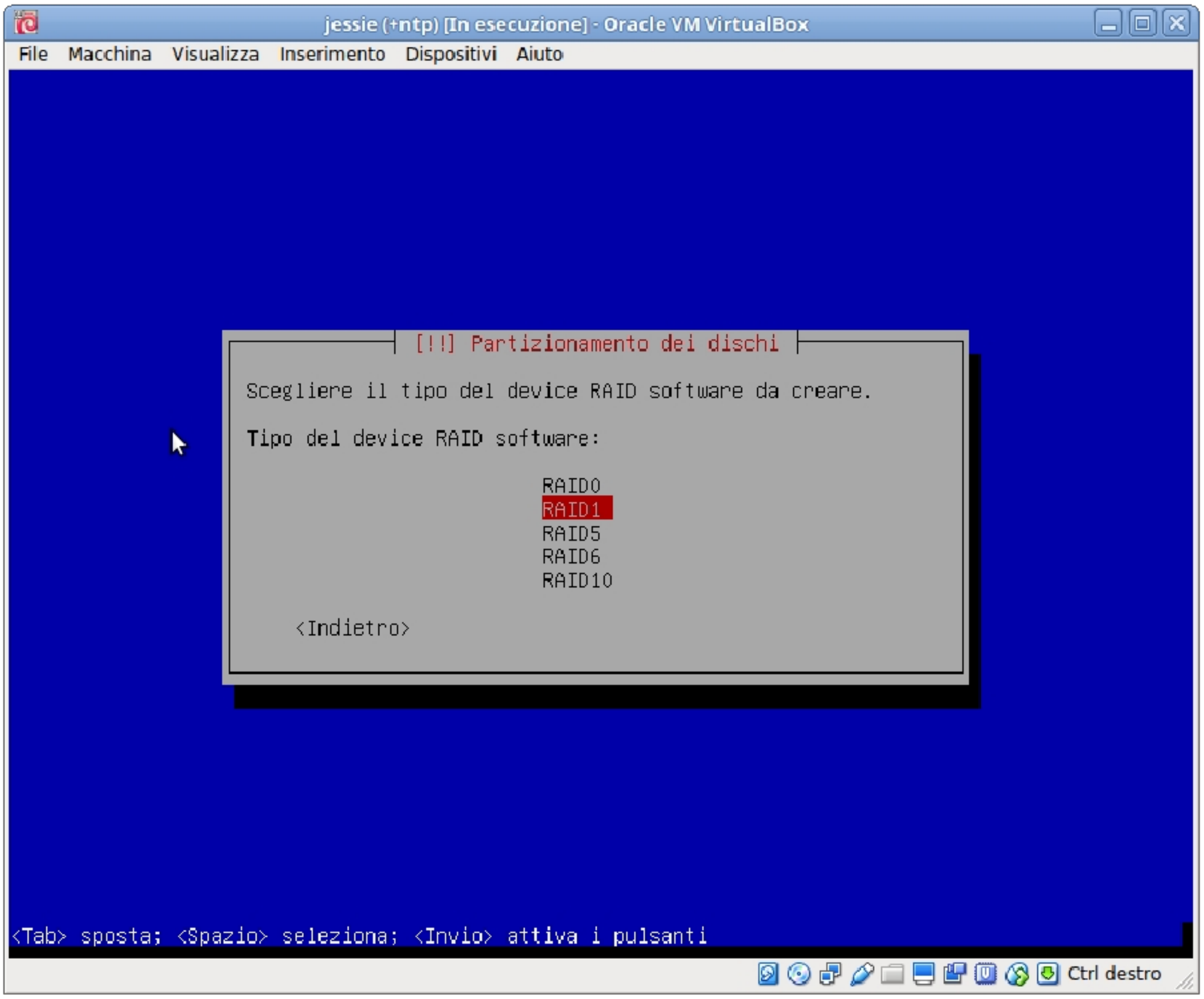
8.1.3 Configure software RAID

Once partitioning is complete, as shown in the figure below, you can move on to software RAID configuration by selecting the second menu item.

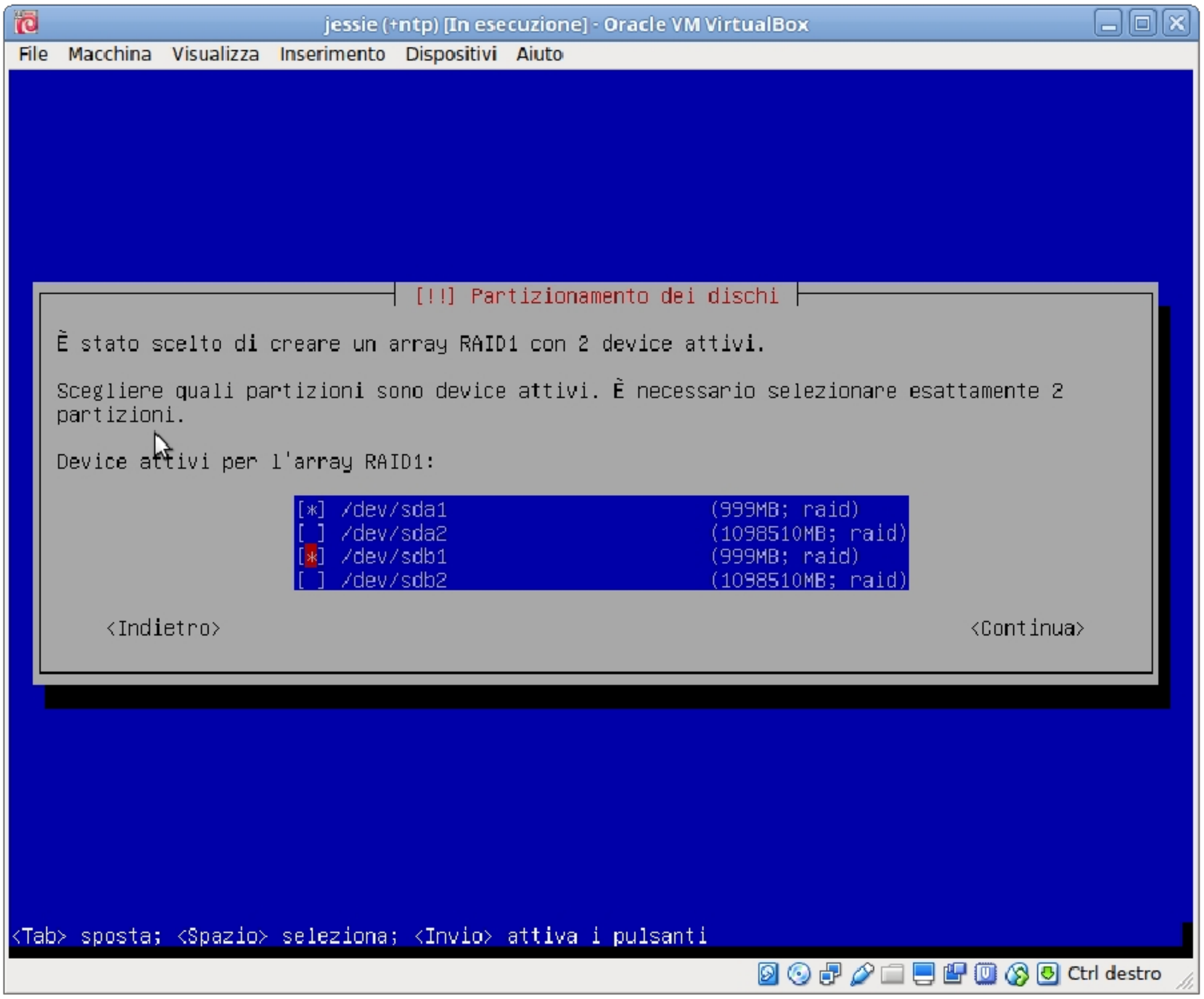


You will be prompted to write the changes to the disks, and then you can move on to the raid configuration by choosing "Create a multidisk device," and then the raid type, which must be RAID1.


jessie (+ntp) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
[!!] Partizionamento dei dischi
Questo è il menù di configurazione del RAID software (o MD, "multiple device").
Selezionare una delle azioni proposte per configurare il RAID software.
Azioni di configurazione RAID software
Creare un device multidisk (MD)
Eliminare un device multidisk (MD)
Termina
<Indietro>
<Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti
Ctrl destro



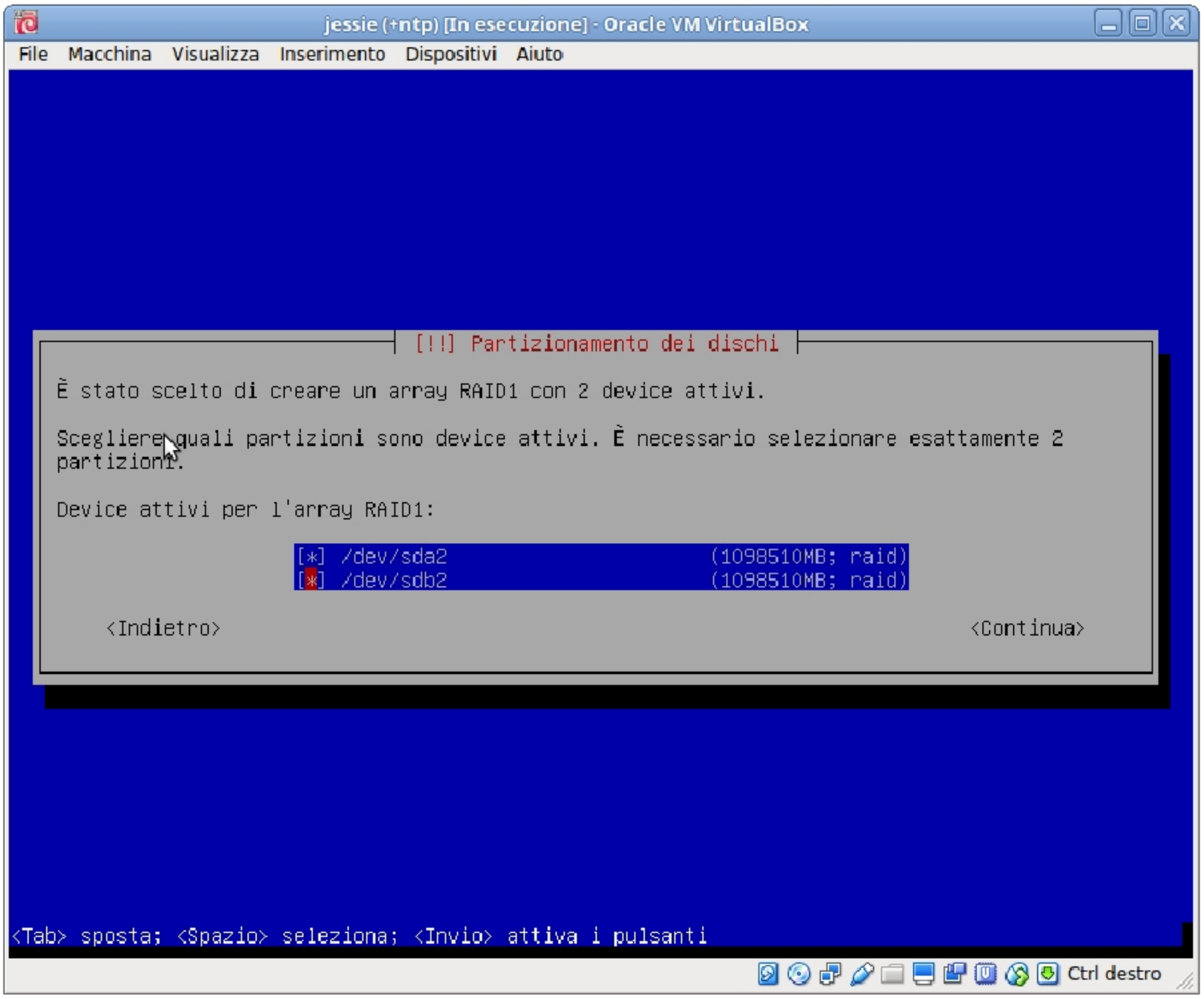
You will then be asked for the number of active devices (accept the default of 2) and the number of spare devices (spare, accept the default of 0), after which you can select the devices that make up the RAID by choosing the first partition of both disks:



Therefore, the sequence will occur:

- When asked "Write changes to storage devices and configure RAID?" select "Yes"
- Select "Create a multidisk device (MD)."
- Select RAID1 from the following menu
- At the prompt "Number of active devices for RAID1 array:" leave the default of 2
- At the prompt "Number of device spares for RAID1 array:" leave the default of 0
- At the Active Devices prompt for the RAID1 array, select `/dev/sda1` and `/dev/sdb1`

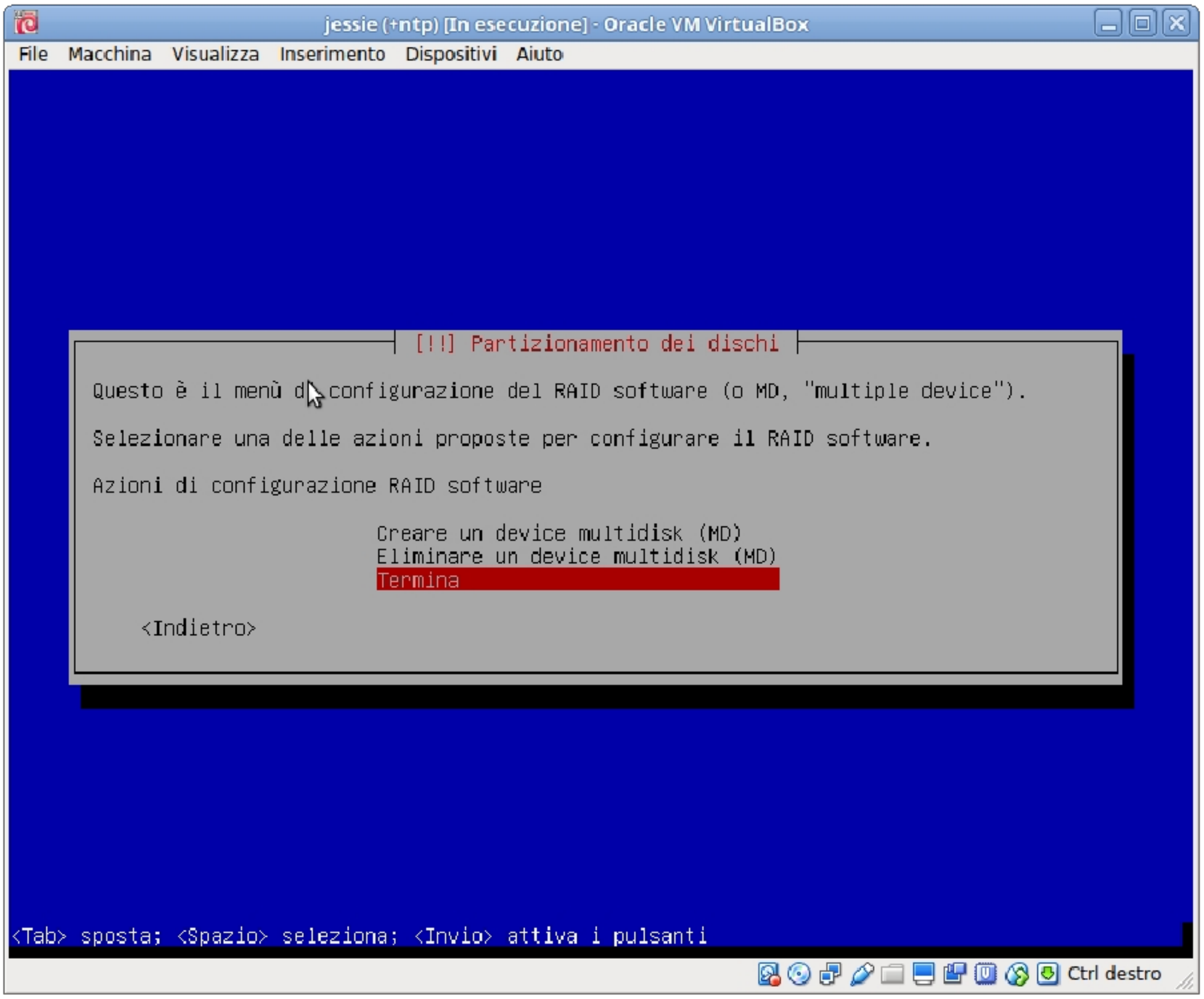
You must then repeat the sequence to create the second RAID1 that will be used for LVM, repeating the previous choices and finally selecting the two remaining partitions.



Therefore, the second sequence will be:

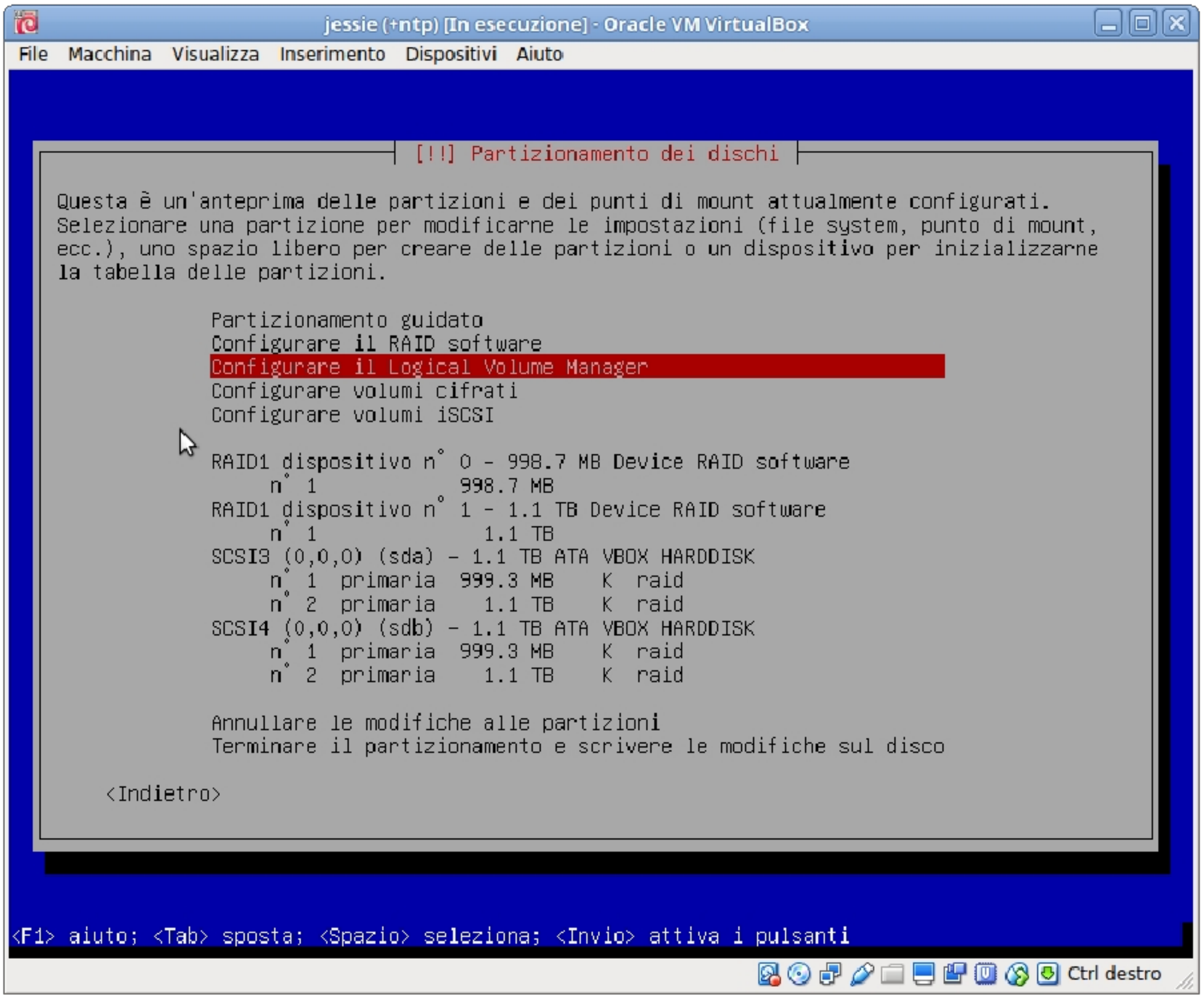
- Select "Create a multidisk device (MD)."
- Select RAID1 from the following menu
- At the prompt "Number of active devices for RAID1 array:" leave the default of 2
- At the prompt "Number of device spares for RAID1 array:" leave the default of 0
- At the Active Devices prompt for RAID1 array, select `/dev/sda2` and `/dev/sdb2`

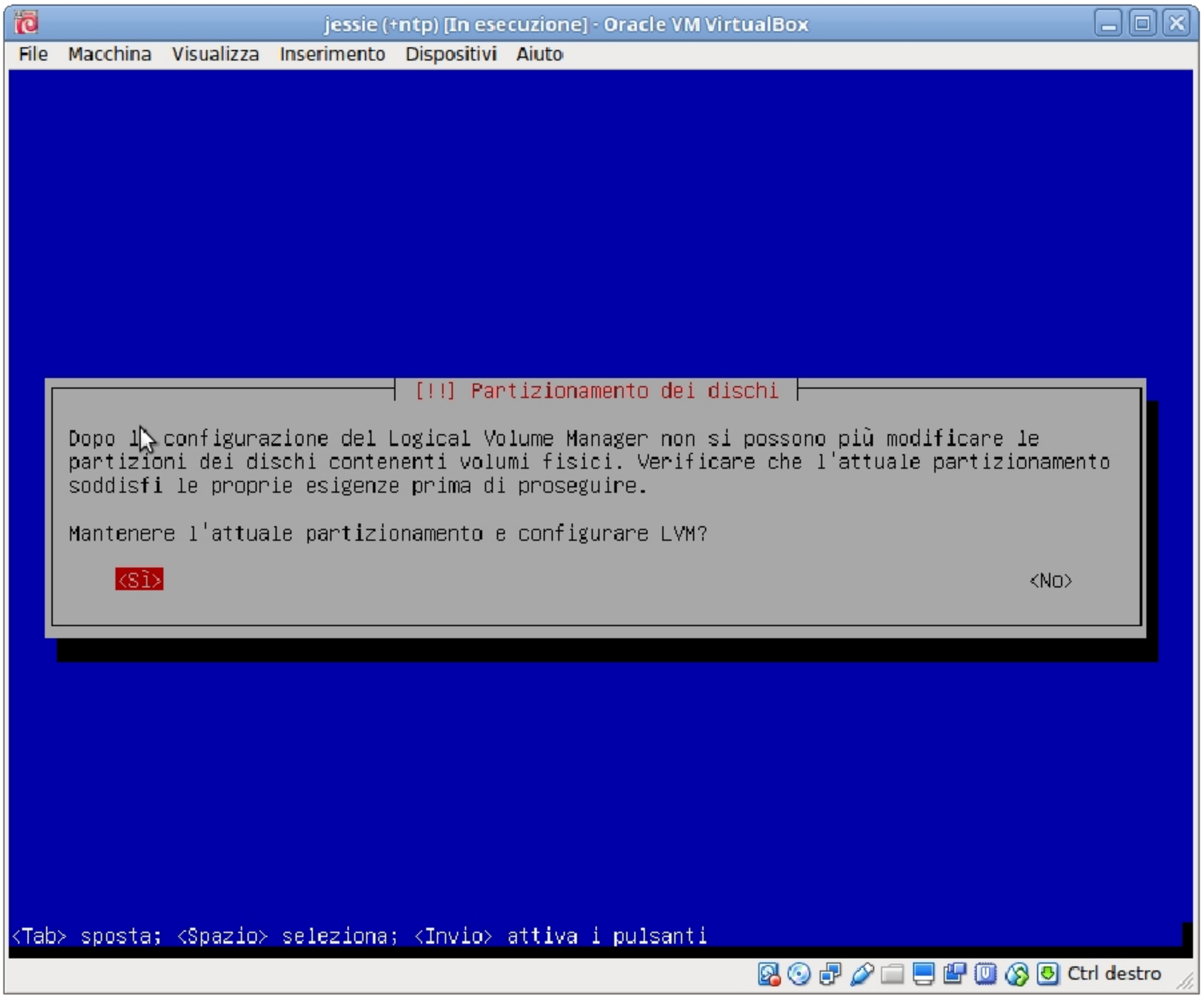
Once this is done the RAID1 setup is complete and you can end it by selecting the appropriate option:



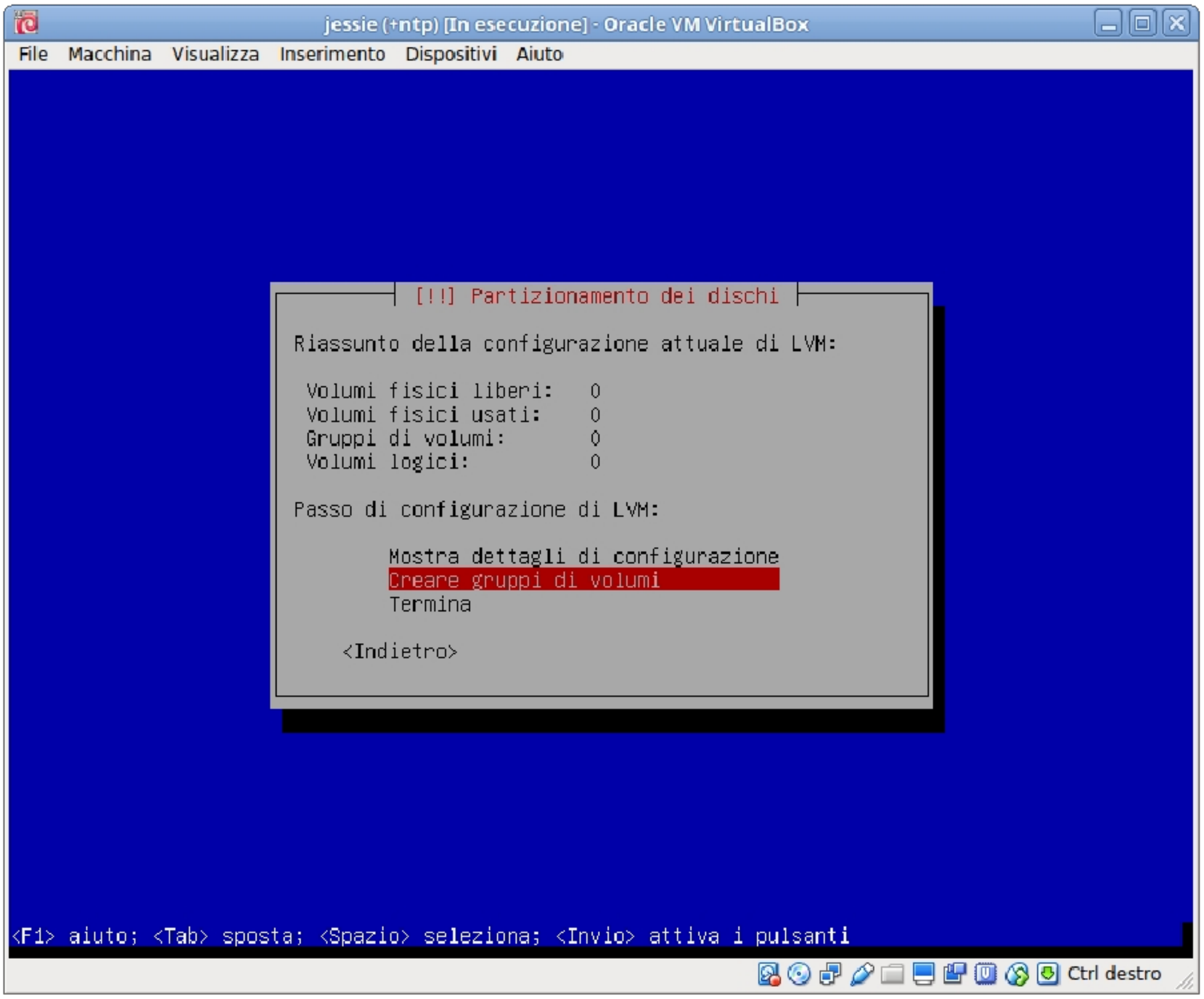
8.1.4 Configure LVM (Logical Volume Manager)

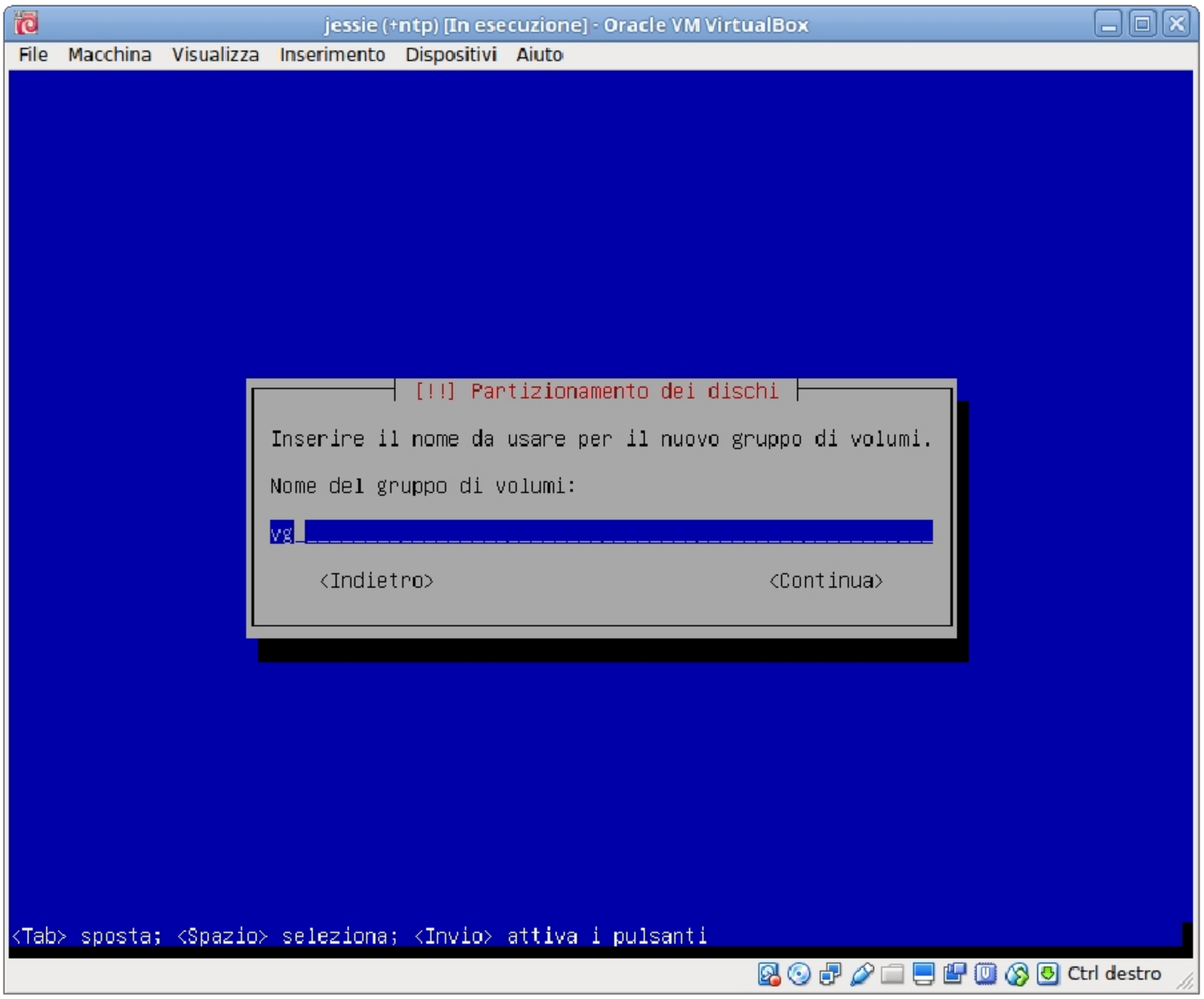
Once the RAID configuration is finished LVM will have to be configured to use the `md1` device on which we have concentrated most of the disk space, from the main screen which at this point will be the following you will have to choose "Configure Logical Volume Manager" and agree to keep the current partitioning:


jessie (+ntp) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
[!!] Partizionamento dei dischi
Questa è un'anteprima delle partizioni e dei punti di mount attualmente configurati.
Selezionare una partizione per modificarne le impostazioni (file system, punto di mount,
ecc.), uno spazio libero per creare delle partizioni o un dispositivo per inizializzarne
la tabella delle partizioni.
Partizionamento guidato
Configurare il RAID software
Configurare il Logical Volume Manager
Configurare volumi cifrati
Configurare volumi iSCSI
RAID1 dispositivo n° 0 - 998.7 MB Device RAID software
n° 1 998.7 MB
RAID1 dispositivo n° 1 - 1.1 TB Device RAID software
n° 1 1.1 TB
SCSI3 (0,0,0) (sda) - 1.1 TB ATA VBOX HARDDISK
n° 1 primaria 999.3 MB K raid
n° 2 primaria 1.1 TB K raid
SCSI4 (0,0,0) (sdb) - 1.1 TB ATA VBOX HARDDISK
n° 1 primaria 999.3 MB K raid
n° 2 primaria 1.1 TB K raid
Annullare le modifiche alle partizioni
Terminare il partizionamento e scrivere le modifiche sul disco
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti
Ctrl destro

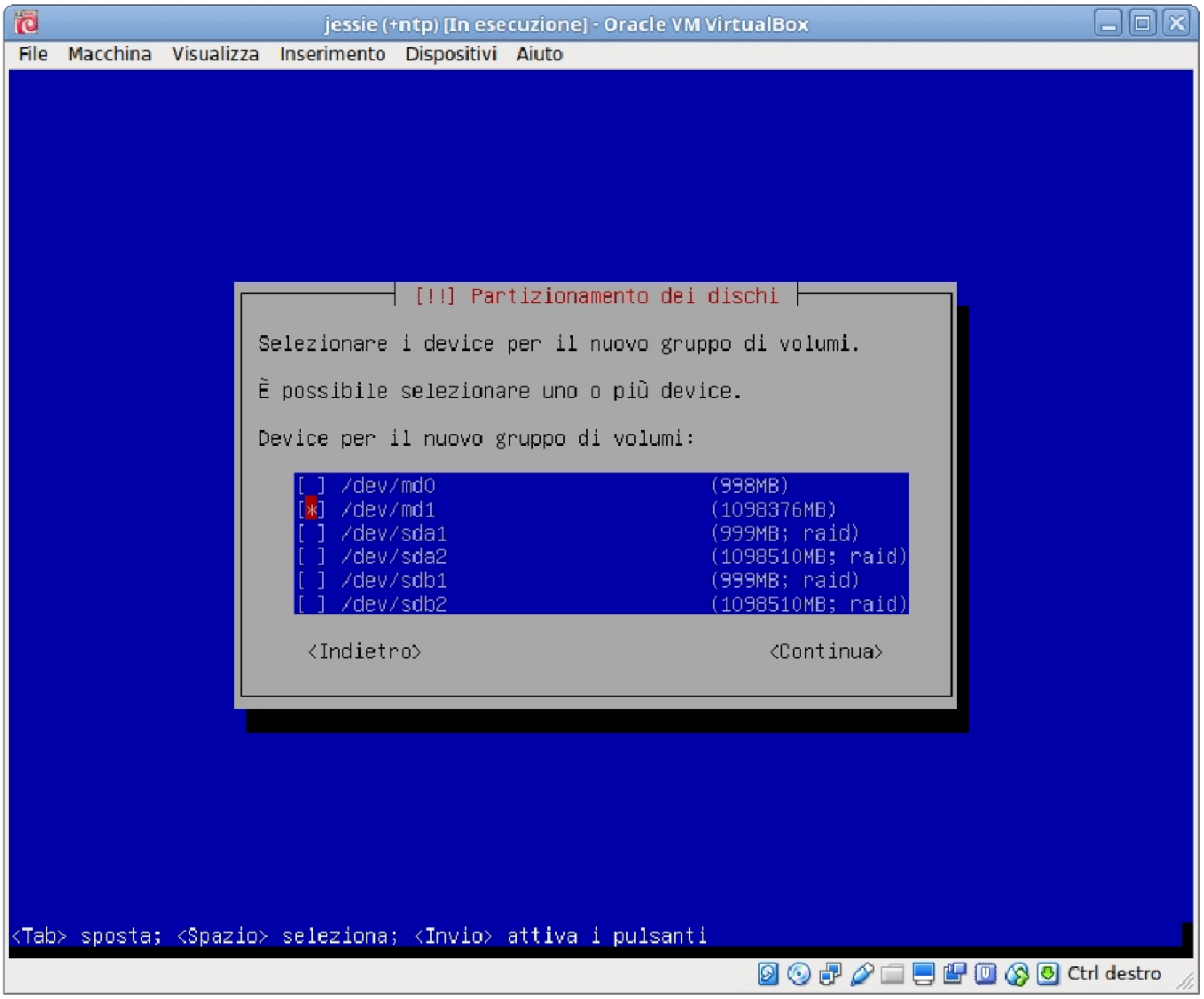


At this point you will have access to the LVM configuration menu, the first step is to create a volume group, choosing the relevant option, and enter its name(e.g. `vg`):


jessie (+ntp) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
[!!] Partizionamento dei dischi
Riassunto della configurazione attuale di LVM:
Volumi fisici liberi: 0
Volumi fisici usati: 0
Gruppi di volumi: 0
Volumi logici: 0
Passo di configurazione di LVM:
Mostra dettagli di configurazione
Creare gruppi di volumi
Termina
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti
Ctrl destro



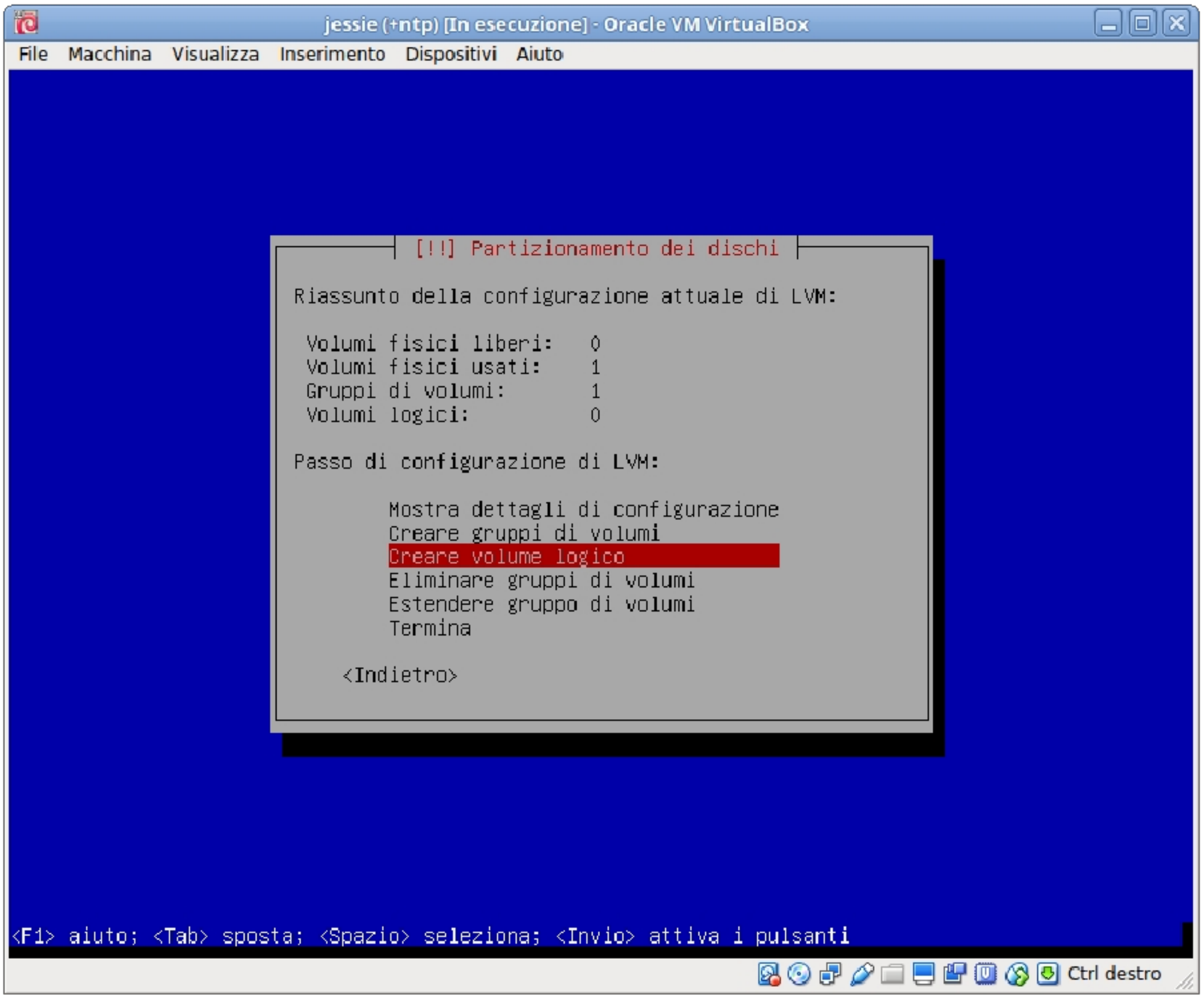
finally, you will need to choose the device (the physical volume) on which to lean for data, which in our case is `/dev/ md1` (you only have to select this):



The sequence of action is therefore.

- Choose from the menu "Create new volume group"
- Set the name of the volume group (e.g., vg)
- Select device `/dev/md1`

At this point you can move on to creating the Logical Volumes, you will need 2, one for the swap and one for the root, which we will call `root` and `swap` respectively. From the LVM configuration menu you will therefore have to choose "Create Logical Volume."

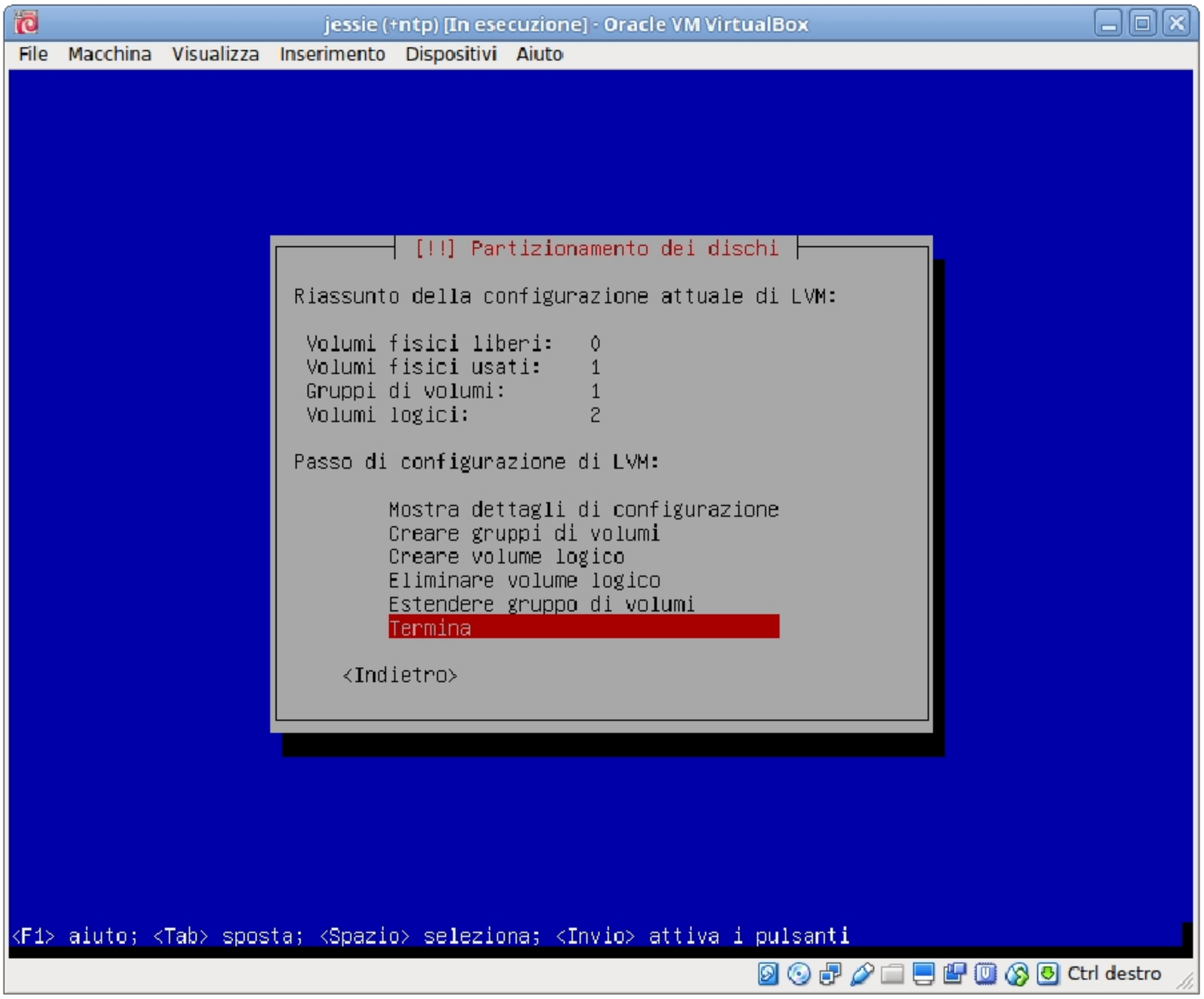


you will be presented with the choice of which Volume Group to use, stuck on the only one available, `vg`, created earlier, continuing you can enter the name of the logical volume and its size. The recommended sizes are a size equal to a quarter of the RAM (but without going over 4G) for `swap`, and a size between 30 and 50G for `root`.

Therefore, the steps are as follows, to be repeated twice, first by swap and then by root:

- Choose from the menu "Create Logical Volume"
- Accept the default for the volume group
- At the "Logical volume name" prompt, enter the name (first swap, then root)
- Enter the chosen size (e.g., first 4G, then 50G)

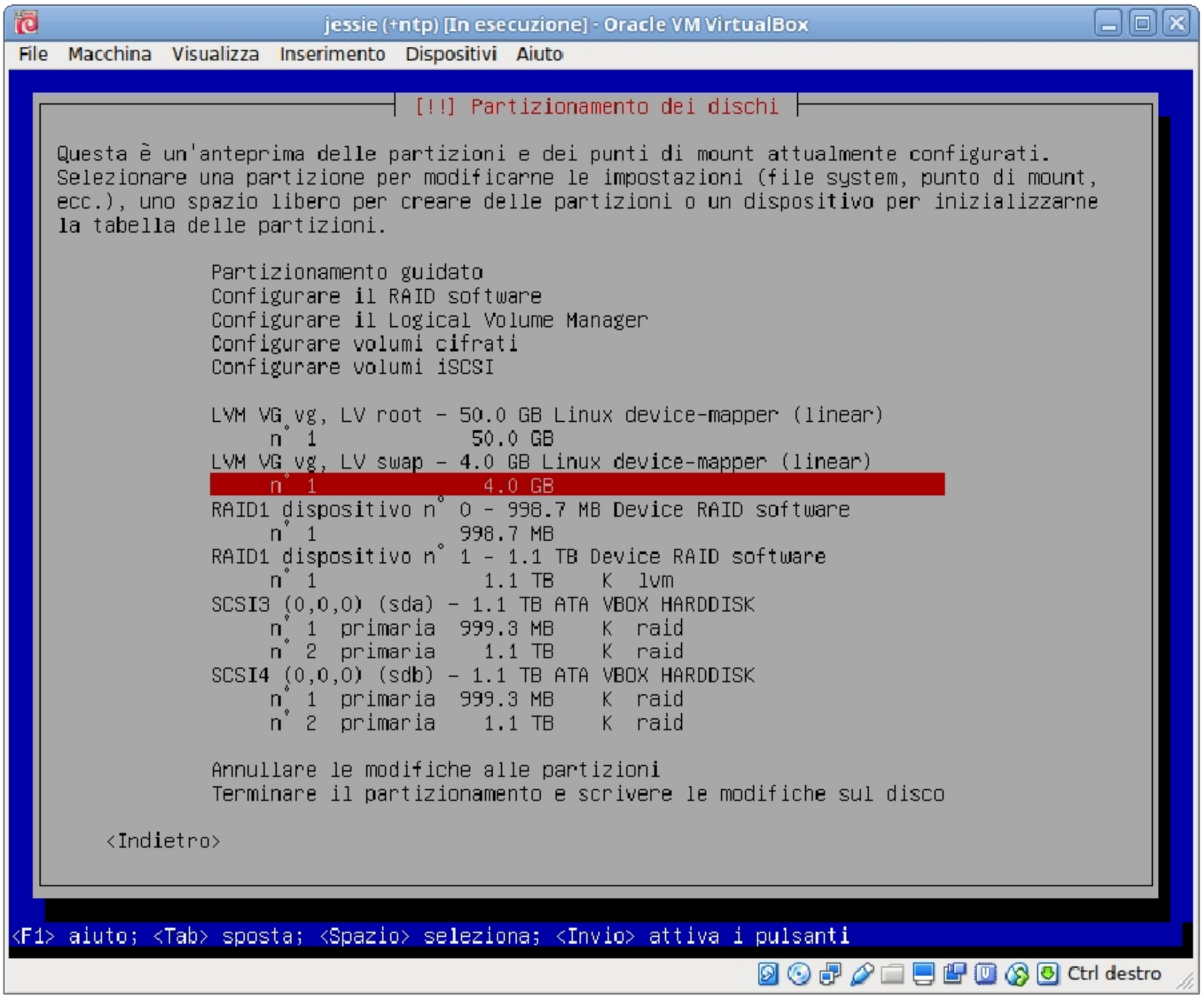
Complete the prompts and you will have the menu screen similar to the following (with one physical volume, one volume group, and two logical volumes) from which you can close the configuration by choosing "Terminate," or verify your choices by choosing "Show configuration details."



8.1.5 Complete disk partitioning and formatting

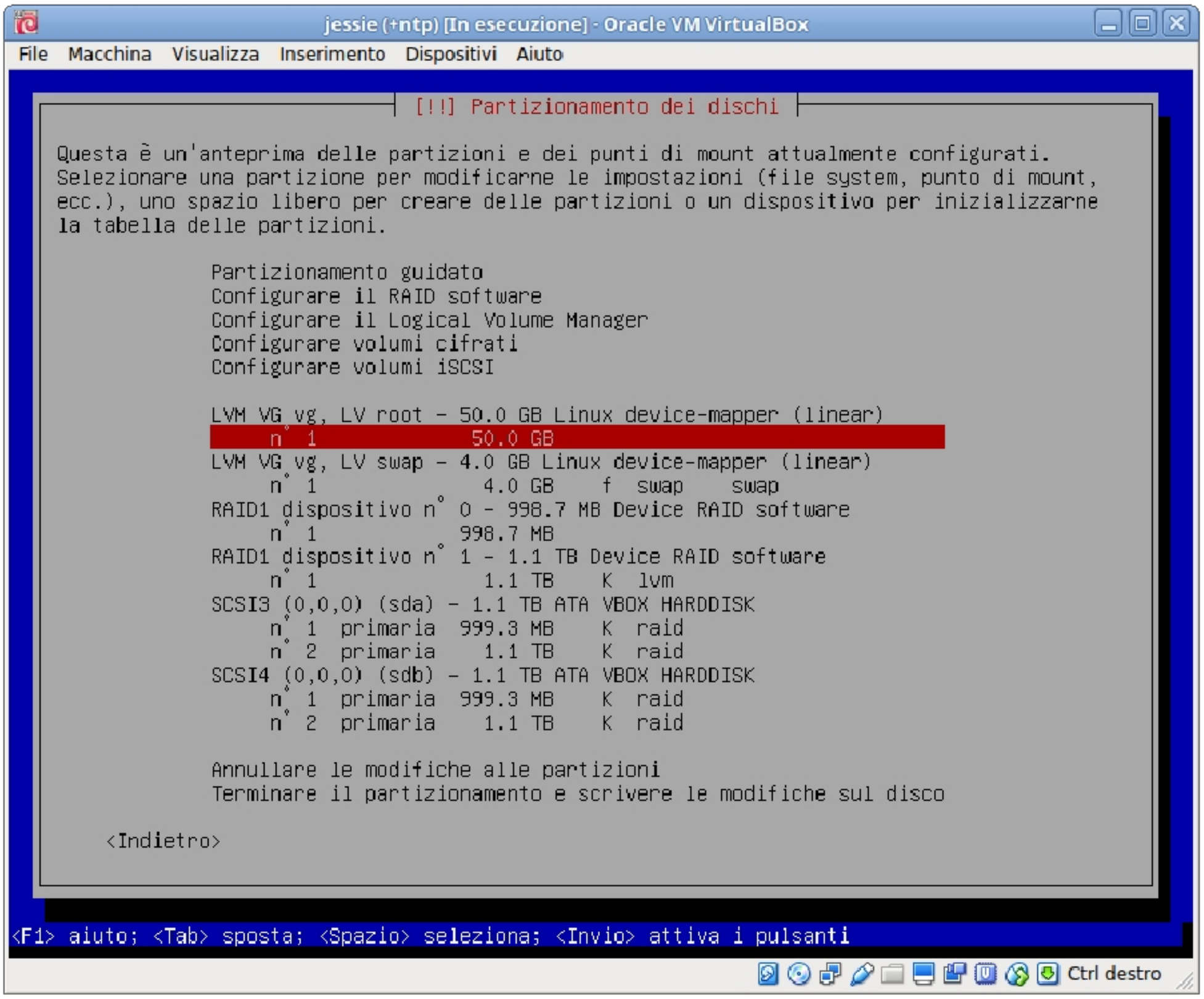
When you have finished configuring LVM you will need to complete the configuration of the disks by indicating how to format the two logical volumes you have just created, and how to format the first RAID1 (`/dev/md0`) that will be used for `/boot`.

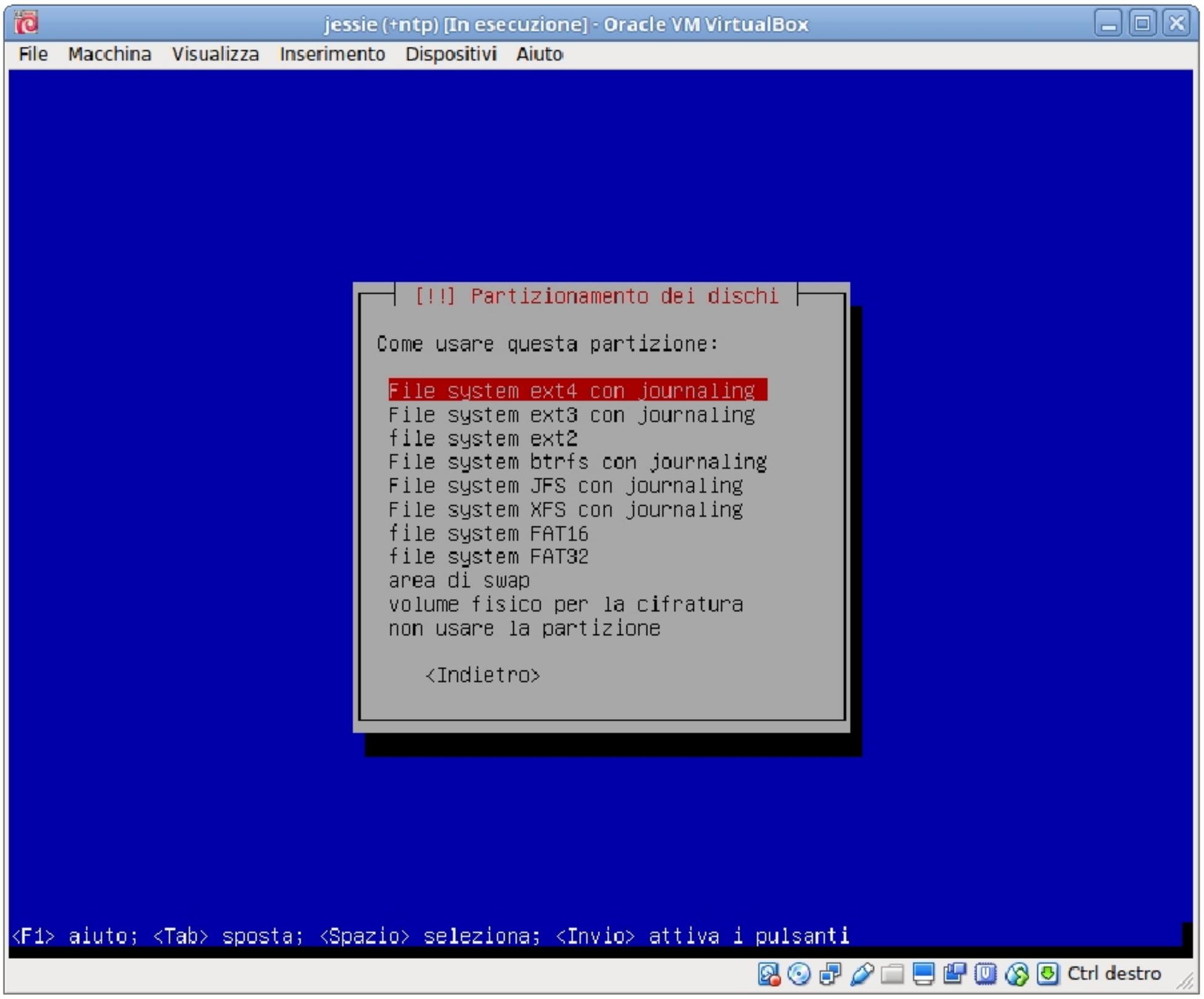
In the case of swap you will have to configure it by selecting the relevant logical volume as in the following image:



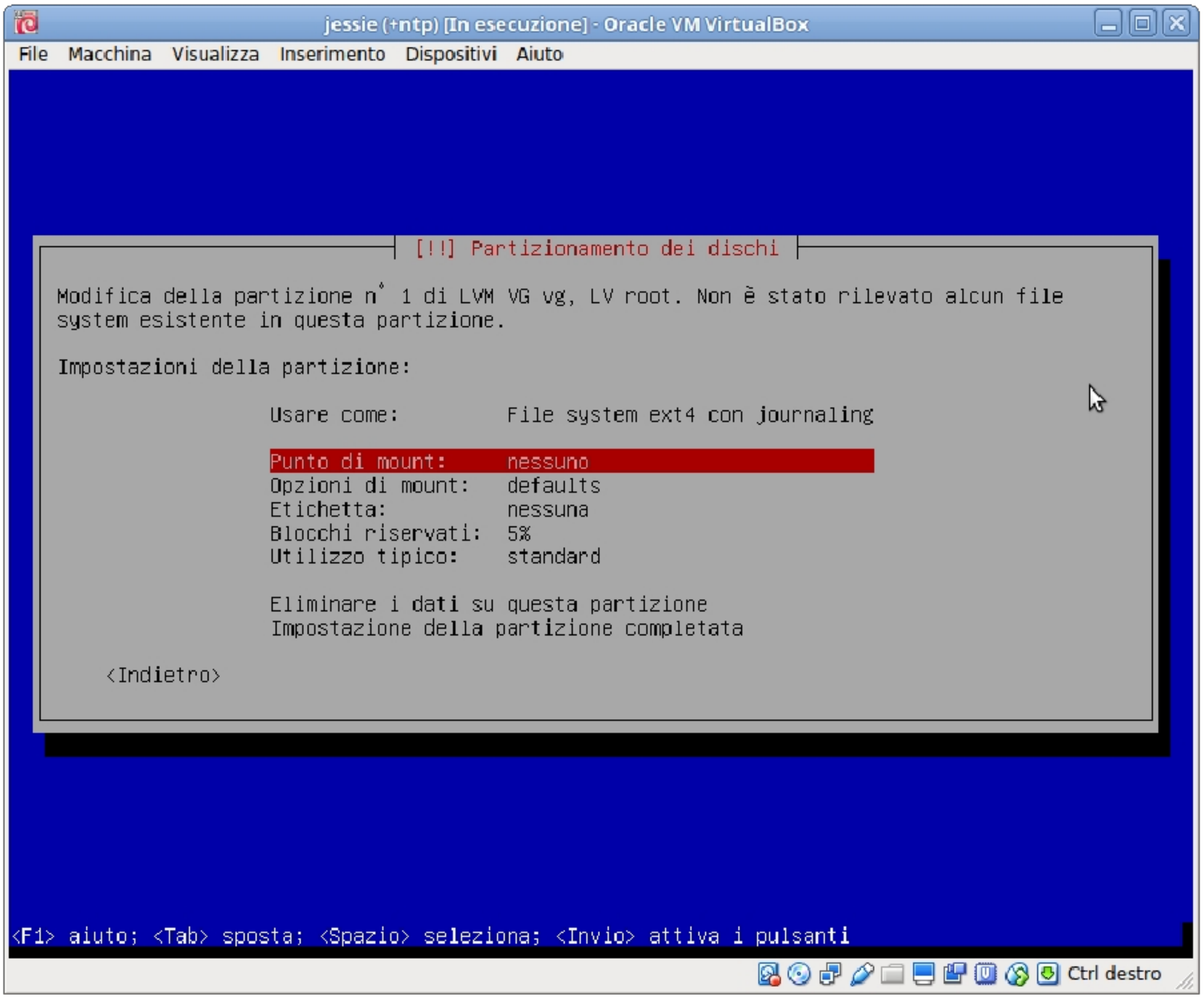
once you choose the volume you will go back to the menu that asks us how to use it, and this time you will need to choose "swap area." In the case of swap, which does not have to be mounted, that is all.

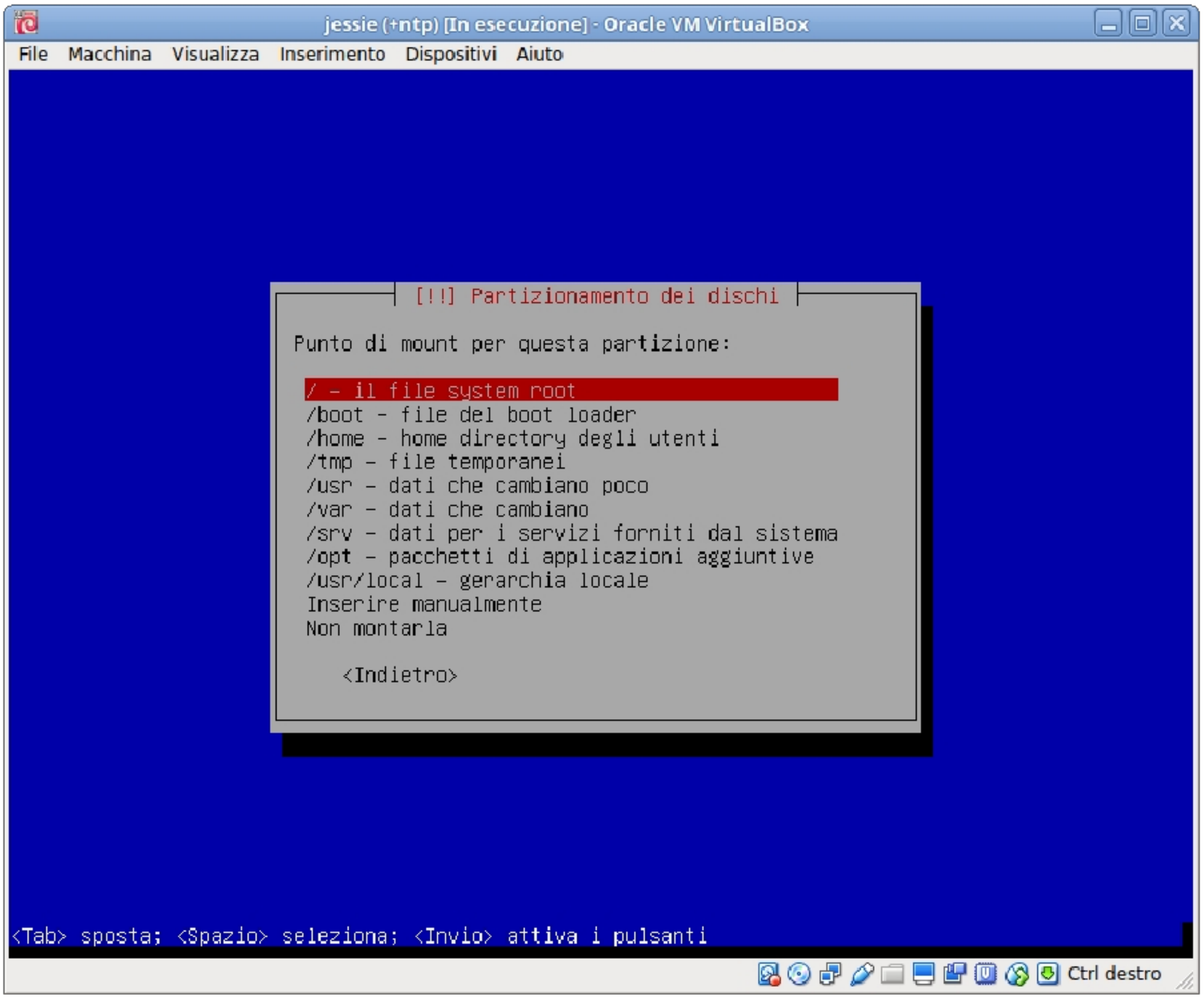
The operation should be repeated to format the root filesystem, again the relevant logical volume should be chosen:


jessie (+ntp) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
[!!] Partizionamento dei dischi
Questa è un'anteprima delle partizioni e dei punti di mount attualmente configurati.
Selezionare una partizione per modificarne le impostazioni (file system, punto di mount,
ecc.), uno spazio libero per creare delle partizioni o un dispositivo per inizializzarne
la tabella delle partizioni.
Partizionamento guidato
Configurare il RAID software
Configurare il Logical Volume Manager
Configurare volumi cifrati
Configurare volumi iSCSI
LVM VG vg, LV root - 50.0 GB Linux device-mapper (linear)
n° 1 50.0 GB
LVM VG vg, LV swap - 4.0 GB Linux device-mapper (linear)
n° 1 4.0 GB f swap swap
RAID1 dispositivo n° 0 - 998.7 MB Device RAID software
n° 1 998.7 MB
RAID1 dispositivo n° 1 - 1.1 TB Device RAID software
n° 1 1.1 TB K lvm
SCSI3 (0,0,0) (sda) - 1.1 TB ATA VBOX HARDDISK
n° 1 primaria 999.3 MB K raid
n° 2 primaria 1.1 TB K raid
SCSI4 (0,0,0) (sdb) - 1.1 TB ATA VBOX HARDDISK
n° 1 primaria 999.3 MB K raid
n° 2 primaria 1.1 TB K raid
Annullare le modifiche alle partizioni
Terminare il partizionamento e scrivere le modifiche sul disco
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti
Ctrl destro

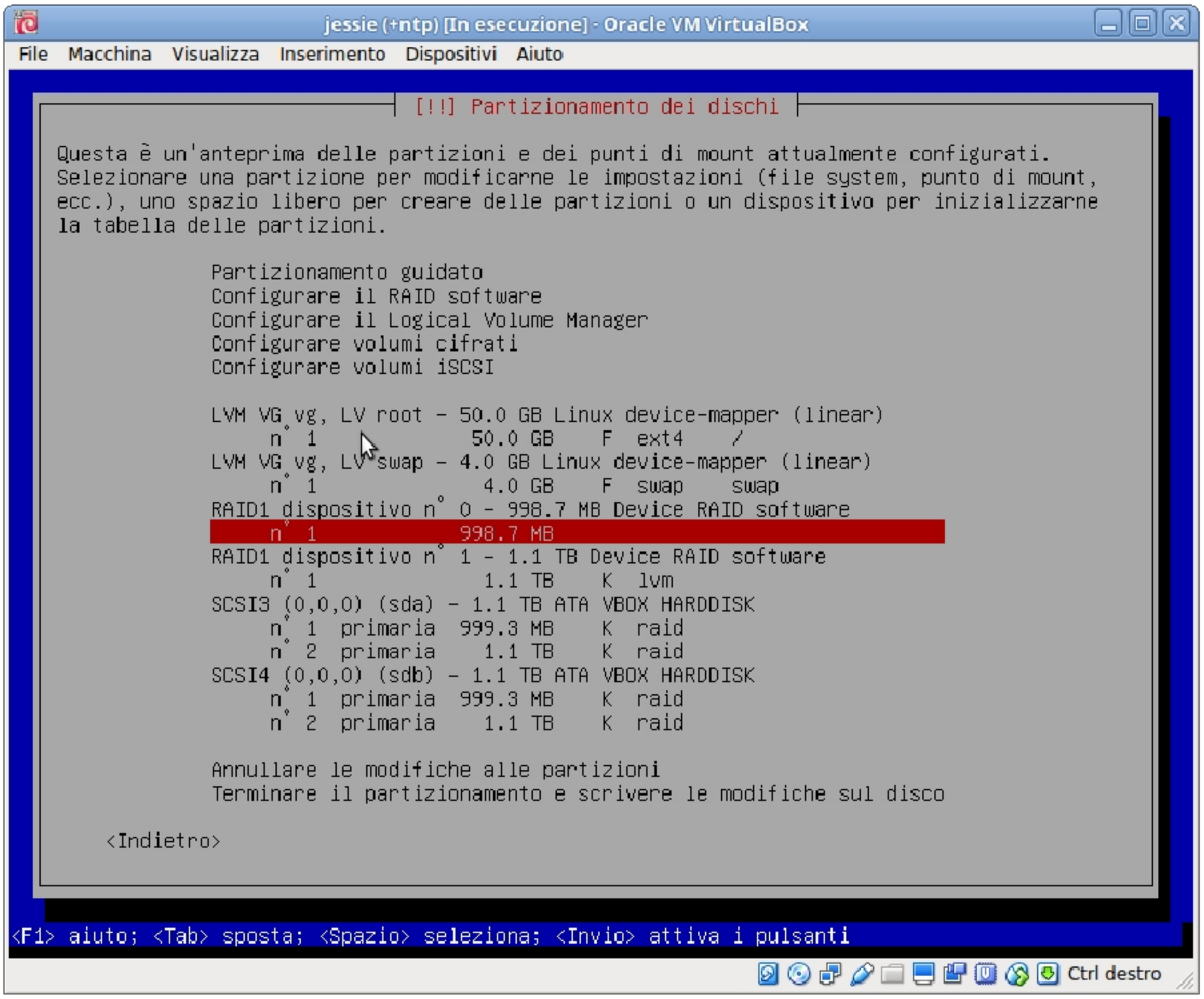


and this time in the "How to use" you will need to select "File system ext4 with journaling," at which point we will also be presented with the choice of "Mount point" and you will need to choose the root:


jessie (+ntp) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
[!!] Partizionamento dei dischi
Modifica della partizione n° 1 di LVM VG vg, LV root. Non è stato rilevato alcun file system esistente in questa partizione.
Impostazioni della partizione:
Usare come: File system ext4 con journaling
Punto di mount: nessuno
Opzioni di mount: defaults
Etichetta: nessuna
Blocchi riservati: 5%
Utilizzo tipico: standard
Eliminare i dati su questa partizione
Impostazione della partizione completata
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti
Ctrl destro



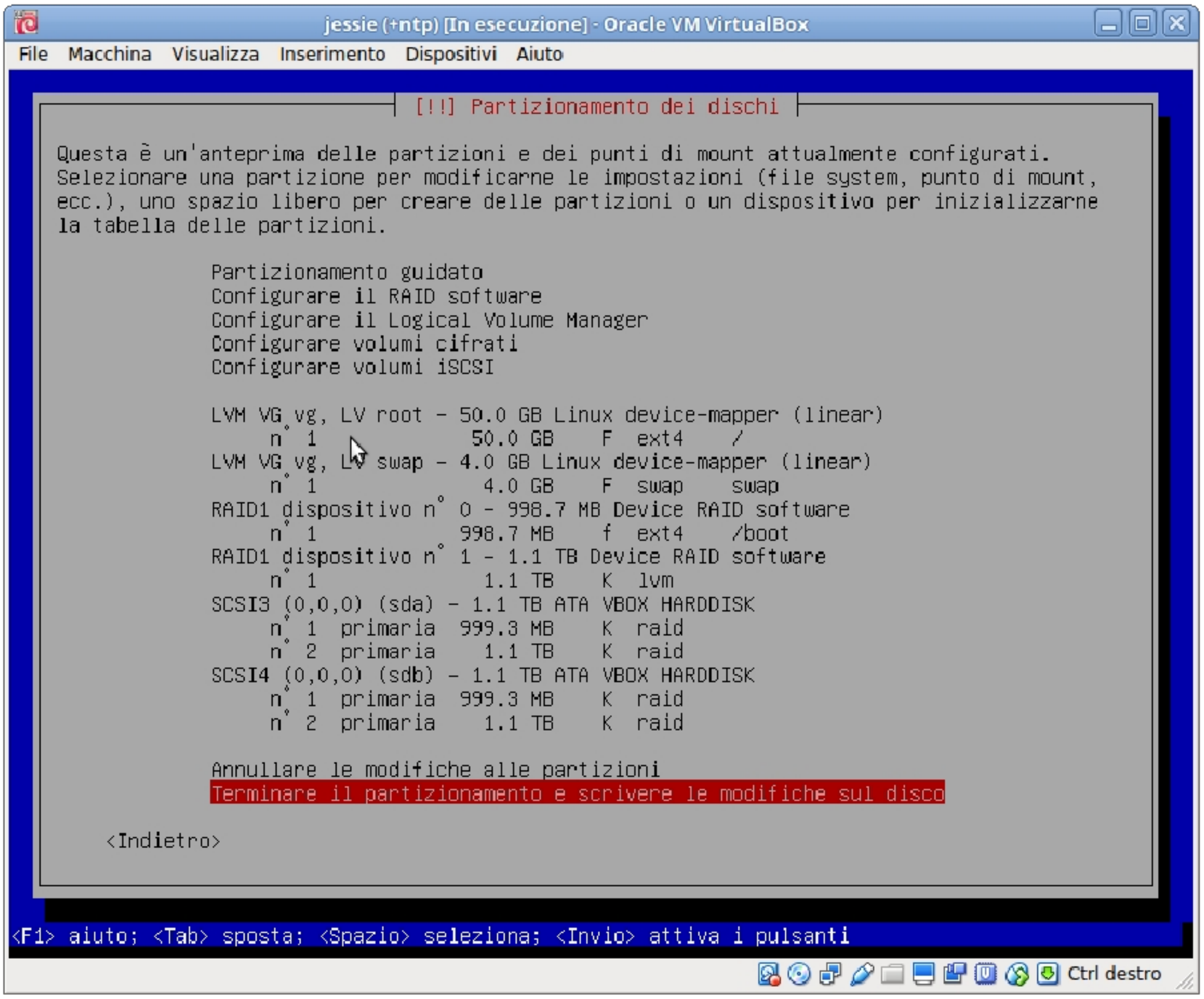
The same operation must be repeated by selecting the device "RAID1 device #0" (see image below) and then still choosing to use as "ext4 file system with journaling" but selecting `/boot` in the "Mounting Point.



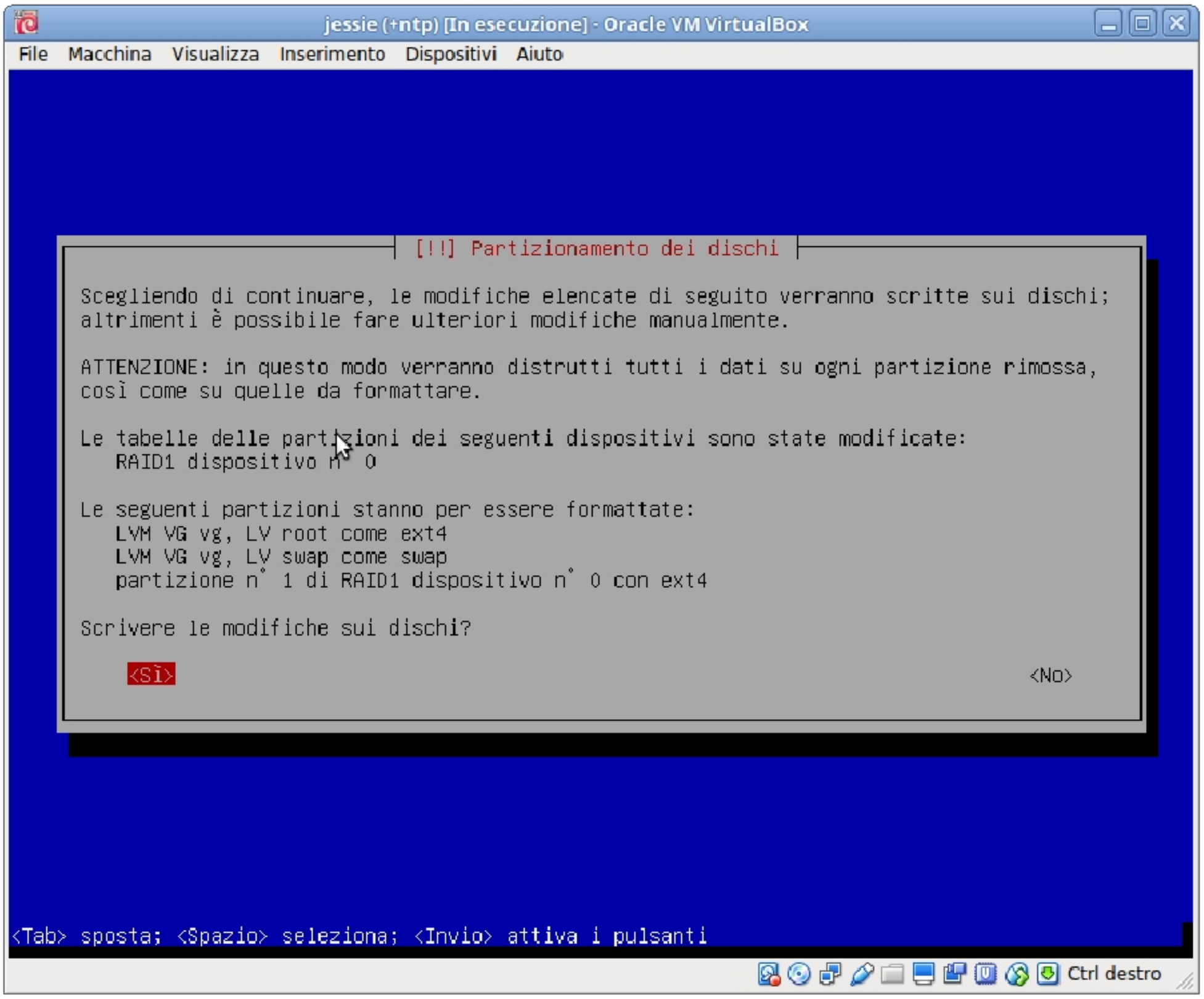
Summarizing the steps are:

- Select the logical volume LV swap
- Under "Use as:" choose "swap area"
- Conclude on "Partition settings completed."
- Select the logical volume LV root
- Under "Use as:" choose "ext4 file system with journaling."
- In "Mount point:" choose "/ - the root file system."
- Conclude on "Partition settings completed."
- Select RAID1 device #0
- Under "Use as:" choose "ext4 file system with journaling."
- In "Mount point:" choose "/boot - boot loader file"
- Conclude on "Partition settings completed."

Once these steps are completed you should have a configuration similar to the one shown in the following image:



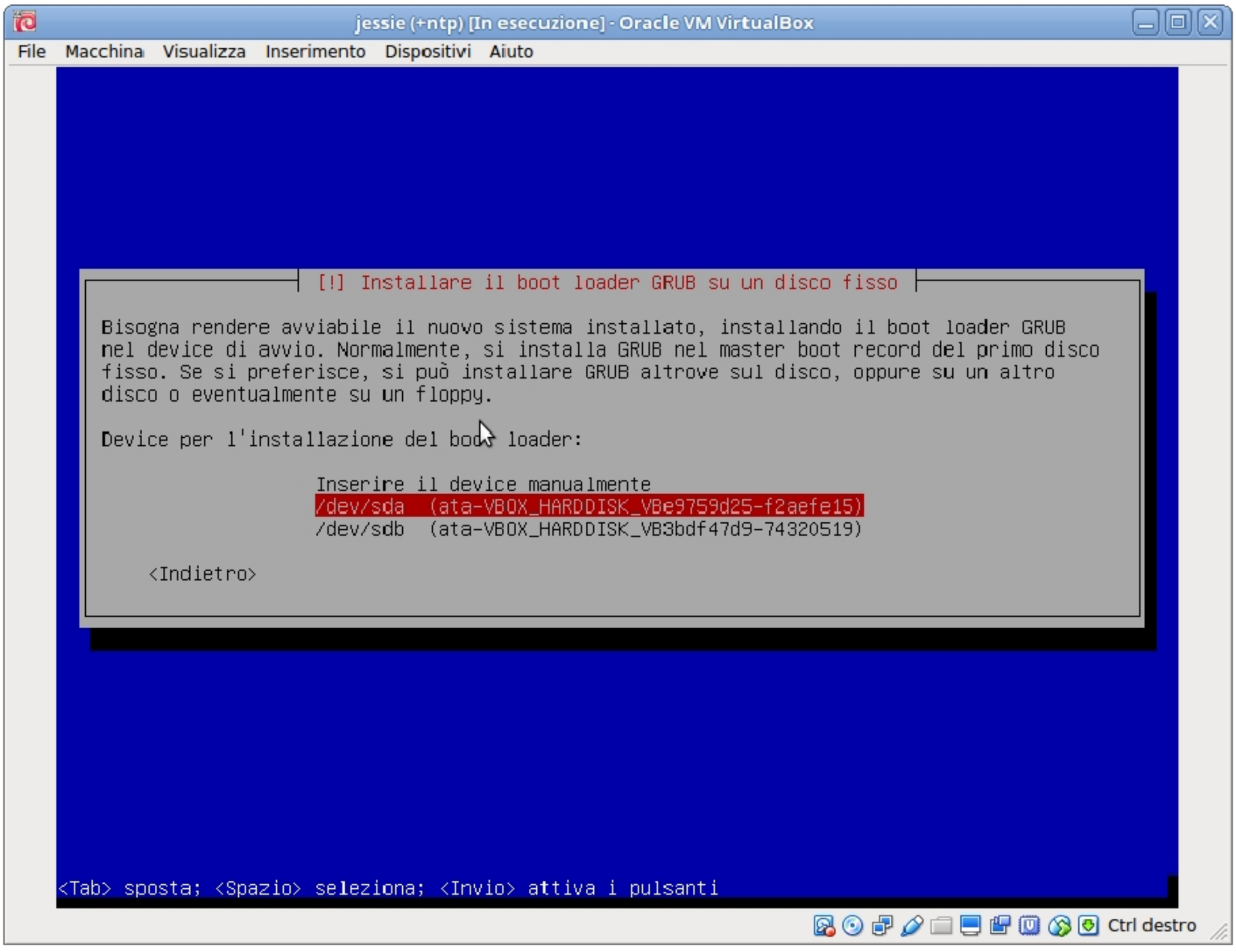
and you can continue by choosing "End partitioning and write changes to disk" and confirming on the next screen:



At this point you can continue with the rest of the installation.

8.1.6 Finalizations

The final screen prompts you to install Grub, choose to install on the first disk, as shown in the figure below:



When you have finished the procedure and installed the server, you must reboot without a CD to verify that the machine restarts. At this point you must then make sure that Grub is installed on both disks, which you do with the commands:

```
grub-install
/dev/sda grub-
install /dev/sdb
```

(it is important that Grub is installed on both disks, otherwise in case of failure of the first one the machine will not restart).

From the terminal, you can check the RAID status with the following command, which if executed shortly after installation will show the progress of disk synchronization:

```
local-user@appiano:~$ cat /proc/mdstat
Personalities : [raid1]
md1 : active raid1 sda2[0] sdb2[1]
      976130880 blocks super 1.2 [2/2]
      [UU]
      [==========>.........] resync = 53.3% (520999104/976130880) finish=140.
↪1min speed=54122K/sec

md0 : active raid1 sda1[0] sdb1[1]
      498368 blocks super 1.2 [2/2] [UU]
```

once the synchronization is complete you will have something like:

```
local-user@appiano:~$ cat /proc/mdstat
Personalities : [raid1]
md1 : active raid1 sda2[0] sdb2[1]
      976130880 blocks super 1.2 [2/2]
      [UU]
```

(continues on next page)

(continued from previous page)

```
md0 : active raid1 sda1[0] sdb1[1]
      498368 blocks super 1.2 [2/2] [UU]
```

8.2 Installation of Proxmox on Debian

This procedure applied to machines for which the RAID controller is not recognized (e.g., Fujitsu PRIMERGY TX1320 M1 servers). Since the Proxmox installer does not support software RAID you will need to use the Debian one, and then switch to Proxmox once Debian is installed. For other cases, the procedure outlined in the *Direct Installation of Proxmox* section applies.

Installation of the 6.x version of proxmox based on Debian Buster is described in detail; on new machines it should no longer be needed, but in case it may also be useful to consult https://pve.proxmox.com/wiki/Install_Proxmox_VE_on_Debian_11_Bullseye to check for any adjustments for the current version.

8.2.1 Basic installation

Start by installing a Debian Buster from a CD, DVD, or USB stick; you have two options for choosing an image:

- Download and install `debian-live-<version>-amd64-xfce.iso` from https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/
- Download and install the netinstall `debian-<version>-amd64-netinst.iso` or the `debian-<version>-amd64-xfce-CD-1.iso` installation order CD from https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/

Installation is the ordinary installation of a Debian base system, but there are cautions to follow regarding network configuration and disk partitioning.

The network must be configured with static IP (it will still need to be reconfigured later from within Proxmox). If you have only one public IP and you are behind a NAT (it is assumed that internet access in that case is handled by a router) the IP of the internal network to which packets from outside are redirected must be left to the fuss-server (if you want reachability of the same remotely). Therefore, use another IP in the internal network used by the router.

If, for example, the router has internal IP `192.168.112.1` and uses the `192.168.112.0/24` network and redirects all traffic from outside to IP `192.168.112.2`, the latter will have to be used on the Fuss Server virtual machine, and you will not be able to use it for the installation. Therefore, assuming that you have put on the same stretch of the network the first interface of the server (it is assumed to be `eth0`) in the installation you can use any other free IP on the network, for example `192.168.112.102`.

For disk partitioning, you need to install on software RAID using LVM in order to be in the same situation as if you were installing Proxmox on a hardware RAID. This part of the procedure is described in detail in the section *Installing Debian on Software RAID* to which we refer.

The procedure is to install with a separate `/boot` (installed directly on the first RAID1, placed on `/dev/md0`) with everything else on an LVM volume (installed on the second RAID1, placed on `/dev/md1`). The sizes of the various partitions and logical volumes therefore are as follows, also illustrated on the page cited above:

- a first RAID1 disk for `/boot` on the order of 1Gb
- a second RAID1 disk as the physical volume of LVM with all the remaining disk space
- A logical swap volume on the order of a quarter of the RAM (but not to exceed 4G)
- a logical volume for `/root` on the order of 30/50G depending on whether or not you also plan to install the GUI.
- no other logical volumes being installed (they will be created later)

8.2.2 Any corrections to the initial installation

With an ordinary installation you should get an already working configuration, and you can go di- retly to the *Preparing to Install Proxmox* section, but some possible post-installation fixes of Debian are as follows:

1. Change the root and local user passwords created during installation (e.g.local-fuss):

```
passwd root
passwd local-
fuss
```

2. Install additional firmwares, only if necessary; copy the firmwares (`*.deb`) to the `/opt` folder and install them with:

```
cd /opt
dpkg -i *.deb
```

3. Edit the network card configuration file, this step is to be performed only if the network configuration performed during installation within the Debian installer did not work correctly, to edit it open the `/etc/network/interfaces` file with any editor, for example by running `vim /etc/network/interfaces`; an example of the file is as follows:

```
# 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
car lo
iface lo inet loopback

# The primary network interface -- WAN
auto eth0
iface eth0 inet static
    address 192.168.112.102
    netmask 255.255.255.0
    192.168.112.0 network
    broadcast 192.168.112.255
    gateway 192.168.112.1
    # dns-* options are implemented by the resolvconf package, if installed
    # dns-nameservers 208.67.222.222 208.67.220.220 8.8.8.8
```

   verify that the network card name (`eth0` in the example) matches the network card detected on the machine by the `ip a` command.

4. if you have changed the interfaces configuration file run the network services restart with:

```
service networking restart
```

5. Modifications to the repositories file (`/etc/apt/sources.list`); this step is to be performed only if oc- runs to insert additional repositories or make corrections from those installed by default by the Debian installer, open the file with `vim /etc/apt/sources.list` an example of the file is:

```
deb http://security.debian.org/ buster/updates main
deb-src http://security.debian.org/ buster/updates main
#
deb http://deb.debian.org/debian/ buster-updates main
deb-src http://deb.debian.org/debian/ buster-updates main
#
deb http://deb.debian.org/debian buster main
deb-src http://deb.debian.org/debian buster main
```

6. Changes to the DNS setting; this step is to be performed only if the network configuration exe- guised during installation within the Debian installer did not work correctly, open the file with `vim /etc/resolv.conf`, a possible example (using the Cloudfare server) is:

```
# Generated by NetworkManager
nameserver 1.1.1.1
```

and one can immediately verify its operation by, for example, pinging to a known server:

```
$ ping www.linux.it
```

8.2.3 Preparation for installation of Proxmox

Once you have completed the basic installation of Debian as described in the *Basic Installation* section. there are a number of preliminary steps to take before moving on to install the Proxmox platform.

Remove unnecessary and/or harmful packages

The following two packages must be removed with commands:

```
apt-get --purge remove network-
manager apt-get --purge remove os-
prober
```

The use of `network-manager` interferes with the configuration of interfaces, it should always be removed, and be sure that it is not possibly reinstalled as a dependency if a graphical interface is installed.

The `os-prober` package is useless and potentially dangerous for any server because it tries to check the contents of all disks to identify which operating systems to boot, including any virtual machine disks that may be active or mounted, so it can also cause heavy filesystem corruptions.

Configure local name resolution

Before going on to install the platform, you need to make sure that the IP address assigned to the machine is resolved correctly in the machine's hostname, otherwise the `pve-manager` service will not start, blocking the installation. For this you need to edit the `/etc/hosts` file installed by default by Debian with:

- In the second line replace IP `127.0.1.1` with the IP assigned to the server, in our case `192.168.112.102`
- In the second line add at the end the additional name `pvelocalhost`

an example of the file, for `server102` machine in domain `dom102.bzn` is as follows:

```
127.0.0.1       localhost.localdomain localhost
192.168.112.102         server102.dom102.bzn    server102 pvelocalhost

# The following lines are desirable for IPv6 capable
hosts.
::1     localhost ip6-localhost ip6-
loopback ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Once the change has been made, the resolution of the local name must be verified; to verify the direct resolution, the command must be executed:

```
getent hosts IP.OF.MY.SERVER
```

For example, with the previous configuration you must have:

```
# getent hosts 192.168.112.102
192.168.112.102 server102.dom102.bzn server102 pvelocalhost
```

For inverse resolution verification run the command:

```
hostname --ip-address
```

And with the previous configuration you must have:

```
# hostname --ip-address
192.168.112.102
```

8.2.4 Installing the platform of Proxmox

Having completed the preliminary configurations in the *Preparing to Install Proxmox* section, you can move on to the installation.

Adding Proxmox repositories

The first step is to add the repository for installation by running the command:

```
echo "deb http://download.proxmox.com/debian buster pve-no-subscription" \
   > /etc/apt/sources.list.d/pve-install-repo.list
```

you must then add the key that signs repository packages by running the command:

```
wget -O- "http://download.proxmox.com/debian/proxmox-ve-release-6.x.gpg" | apt-key␣
↪add -
```

Platform installation

Once the repository data has been updated, the first step is to install the updated packages provided by Proxmox:

```
apt update && apt dist-upgrade
```

you need to wait for the download and installation to complete; it can take up to 15 minutes.

Installing Proxmox packages

Once the packages present have been updated, one can move on to the installation of the platform by installing the necessary with the command:

```
apt install proxmox-ve postfix open-iscsi
```

in the postfix configuration choice you can answer "internet site".

Cleaning operations

The Debian kernel is no longer needed, but when you do updates it downloads that too, so you can remove it with (check which version is actually the one installed):

```
apt remove linux-image-amd64 linux-image-4.9.0-3-amd64
```

Reboot on the Proxmox platform

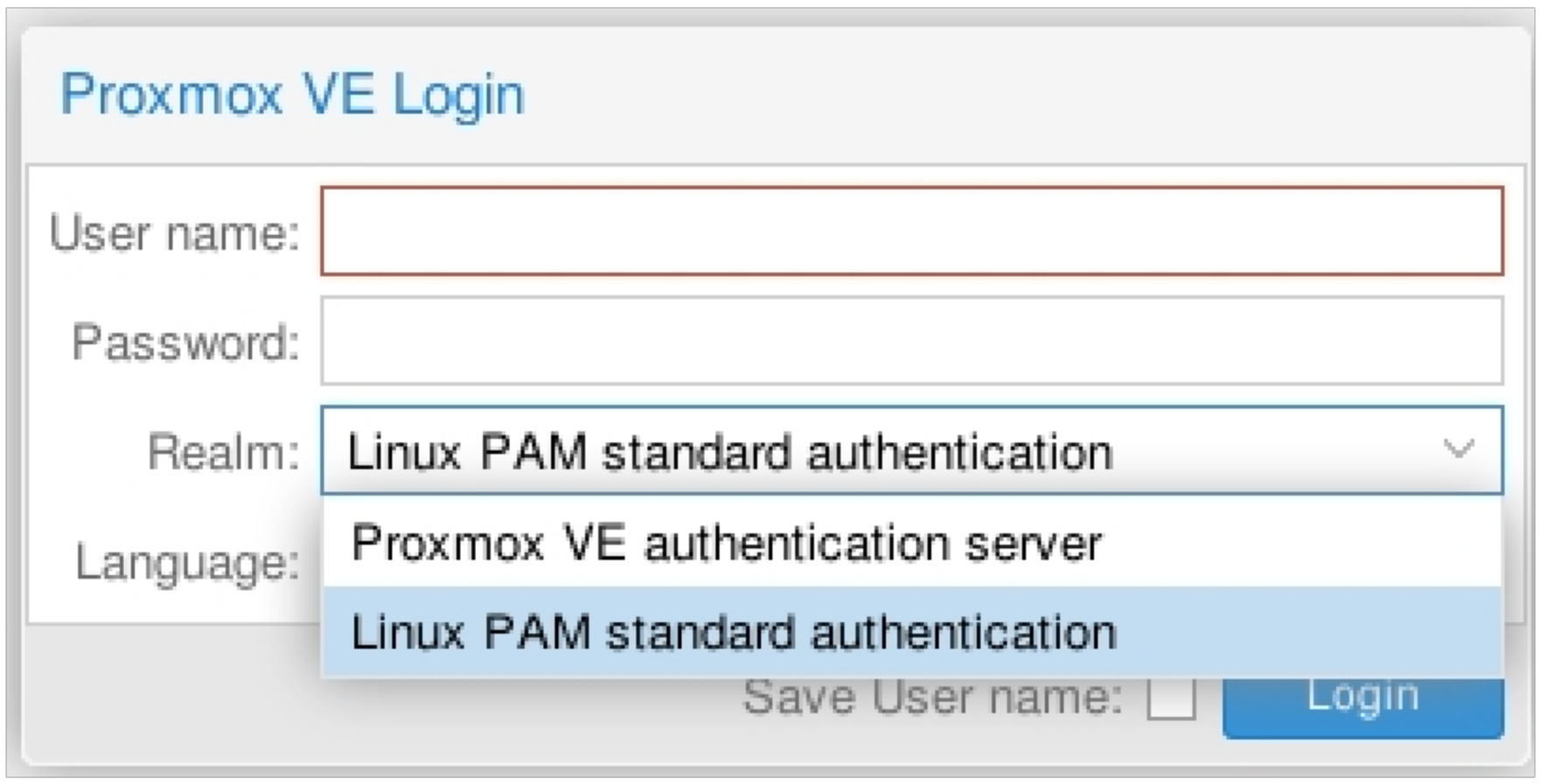
Once you have done the previous steps you can reboot, to be on the safe side you can still run an `update-grub` verifying that the Proxmox kernel (which has the suffix `pve`) appears in the list of kernels. In case you have installed Debian on software RAID1, verify that `grub` is installed in the on both disks, you can check the

thing (and possibly correct the installation) by running `dpkg-reconfigure grub-pc` selecting the two disk devices.

Once the server is restarted, one can connect to the management web interface with the address:

https://IP.DEL.MIO.SERVER:8006

you will get a login window like the following:



must be selected as the "Realm," as in the figure, "Linux PAM standard authentication," and you will be able to connect using the credentials of the `root` user (by entering `root` as the username and its password in the "Password").

The following no-subscription window will appear, to which you can give OK without any problem.



8.2.5 Finalization of the platform

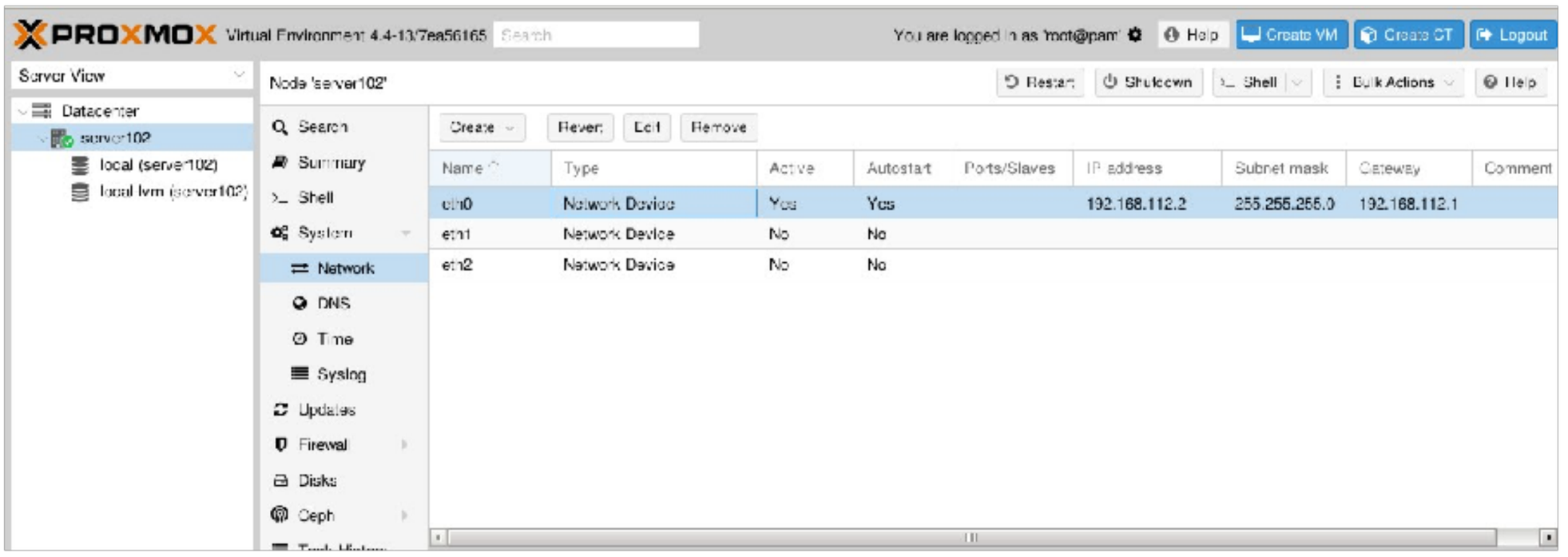
Switching from Debian to Proxmox leaves some configurations to be adjusted compared to the direct installation of the latter. These are the steps to make the necessary adjustments.

Reconfigure the main network interface for bridge use.

We log in from the web interface and access the network configuration section with the following actions:

- Click on the Node (e.g., "server102") in the first panel
- Click on "Network" in the second panel

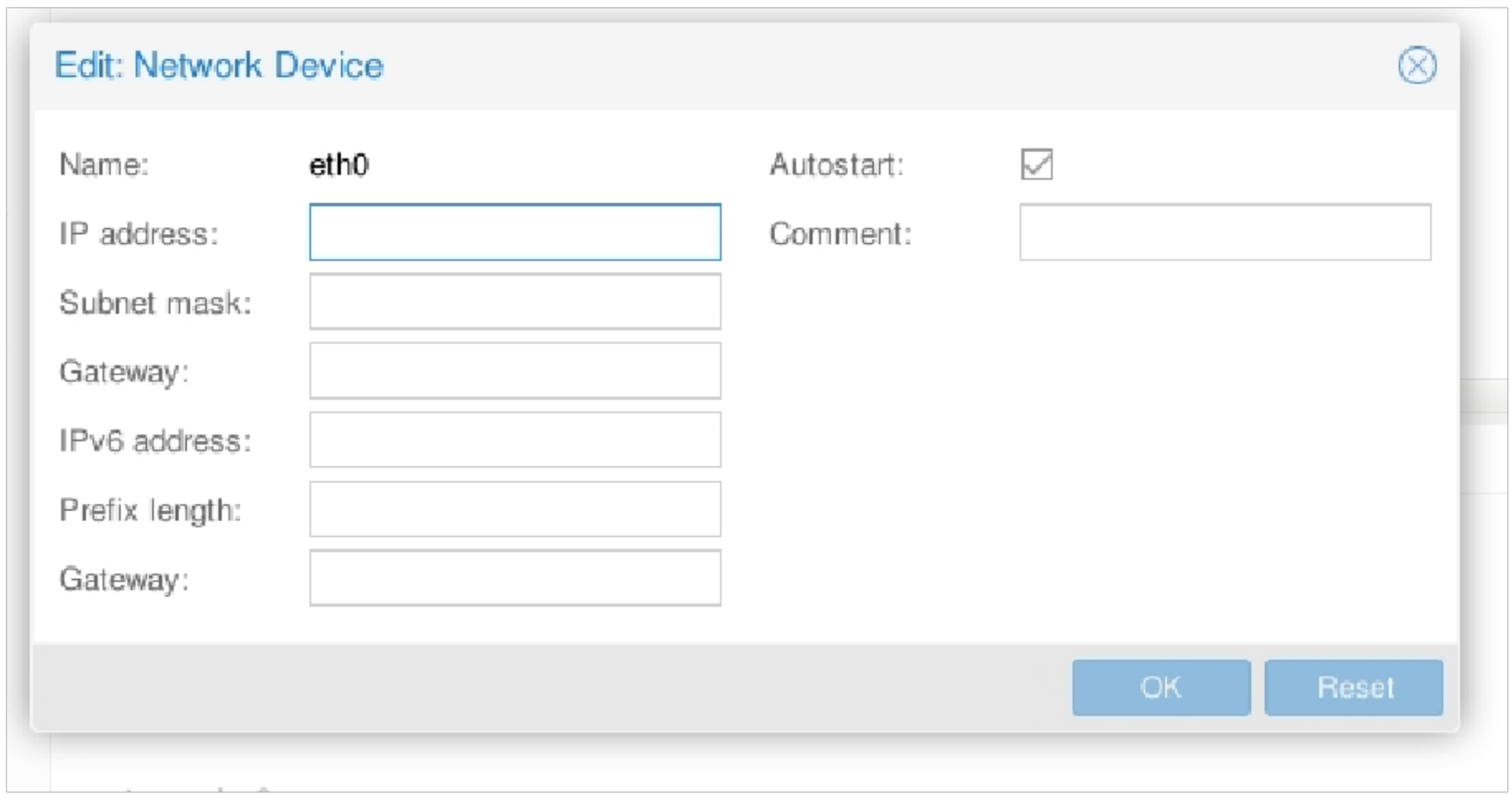
obtaining the following screen:



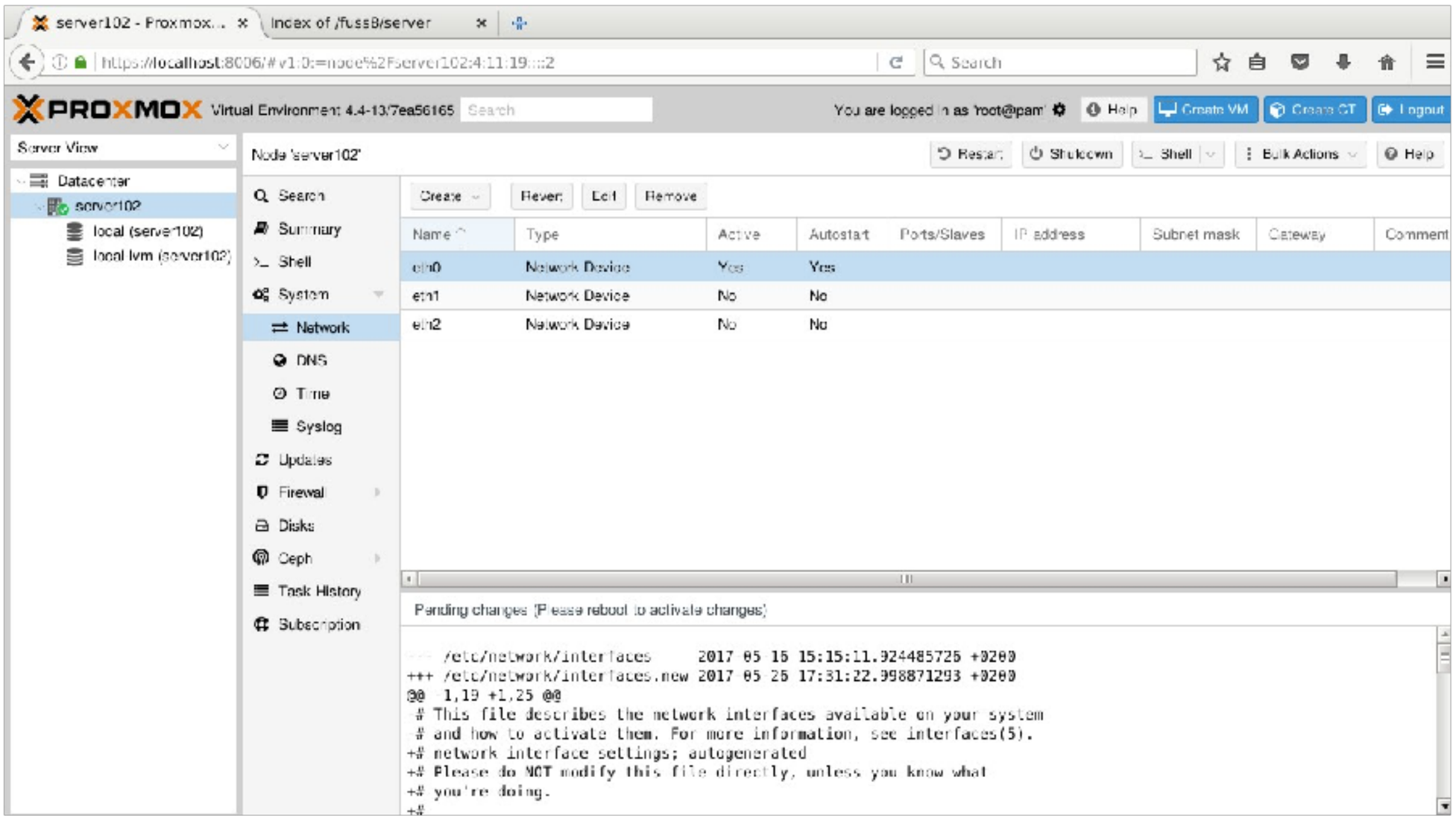
From the network configuration section we will need to delete the `eth0` configuration, which will then be replaced by the `vmbr0` configuration, with the following actions:

- Double click on eth0
- Delete all contained fields and press "OK" the

window should look like the following:



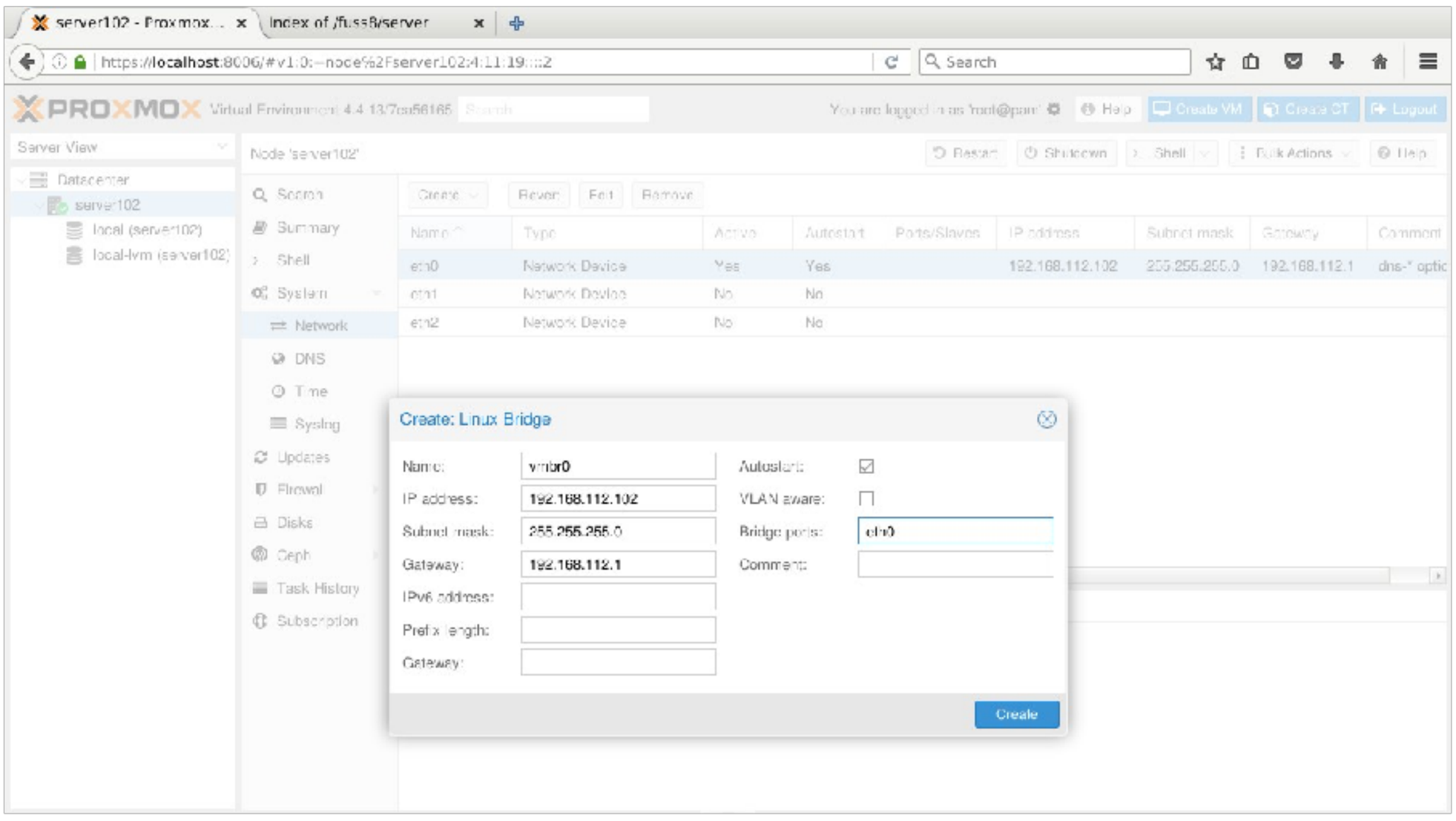
saving the network configuration will result in the following:



At this point we can move on to create the `vmbr0` bridge, we press the "Create" button and from the menu we select "Linux Bridge," a configuration interface will be proposed where you will need to fill in the fields:

- *IP address*: put the same address that was used for eth0
- *Subnet mask*: put the same one that was used for eth0
- *Gateway*: put the same address that you had used for eth0 (the one of the router)
- *Bridge ports*: put `eth0`

an example of configuration is shown in the following image:



to activate the new configurations you need to restart the server, you can do this directly from the "Restart" button.

Create the Logical Volume of the data pool for thin-lvm storage (local-lvm)

The first step is to check with `vgdisplay` how much free disk space is on the LVM volume group (`vg` if you followed the previous instructions):

```
# vgdisplay
...
  Alloc PE / Size       12782 / 49.93 GiB
  Free PE / Size        18897844278 / 788.13 GiB
...
```

Verified the available space we create the logical volume `given` for the pool; it is prudent to leave a lung of free disk space for possible extensions so we will not take all the available space. In case the command:

```
lvcreate -L 715G -n data vg
```

will create a 715 Gb volume, at which point you can mark the new volume as a pool for *thin provisioning* with the command:

```
lvconvert --type thin-pool vg/data
```

Warning: `data` is the name of the logical volume for the pool, you can use any name but this is the one used by default by the Proxmox installer. Instead `vg` is of the volume group that you used in the examples shown in the section *Installing Debian on Software RAID* , in the case of the Proxmox installer this is usually `pve`.

Set up the logical volume for thin provisioning from the Proxmox interface (Datacenter->Storage->Add->LVM-Thin) new storage is added, they will be prompted in a window:

- ID (use local-lvm for consistency with default Proxmox installer)
- Volume group: select from the drop-down menu (or directly write the one used, e.g. `vg`
- Thin pool: write `date` or select it from the drop-down menu (will appear after volume group is set)
- the other fields should not be touched

8.2.6 Final adjustments

It is not required for operation, but a Desktop Environment (xfce4) with a Display Manager (lightdm) and more advanced Terminals than the standard ones can be installed with the command:

```
apt-get install xfce4 lightdm xfce4-terminal gnome-terminal
```

As a browser you can install Firefox with the command:

```
apt-get install firefox-esr
```

8.3 Direct installation of Proxmox

For servers where the RAID controller is recognized, the Proxmox platform can be installed directly; an ISO image that can also be written to a thumb drive can be downloaded. The image is available from the page:

https://www.proxmox.com/en/downloads/

8.3.1 1. Choice of disk space allocation on the installer.

When installing Proxmox from the ISO image you need to choose the disk space allocation. This is done in the Target Harddisk screen (the second one, right after accepting the license); you select as values:

- **swapsize** 4 (4G swap)
- maxroot 30 (30G root, contains only the system)
- **maxvz** - (in this way all the rest of the disk will be placed in the LVM thin-pool)
- **minfree** 50 (let's leave a lung of 50G)

> **Please note:** with this choice, the local storage (marked `local`, associated with the `/var/lib/vz` directory) will have only the root disk space available, which is sufficient to hold the CD iso images for installations; all the space not explicitly allocated is left for virtual machine installations.
>
> If you want to dump the virtual machines to the local disk (dumps could be performed on NAS via NFS, obviously with significantly lower performance), you must instead increase the value of the previous **minfree** parameter, so that you can then create an additional logical volume on which to create a filesystem to dedicate the dumps (the size will have to match the space you plan to use for the virtual machines).

8.3.2 2. Network configuration

The network configuration that is done by the Proxomox installer on the ISO image is static anyway, even when the IP address is obtained from a DHCP server, in which case you need to make sure that the IP you are going to use is out of the range of any DHCP, occur so as not to create possible future IP conflicts. It is preferable to make a manual setting, but the configuration can still be changed later.

For the choice of IP, what was also said about installing Debian applies; if you have only one public IP and you are behind a NAT (it is assumed that Internet access in that case is handled by a router) the IP of the internal network to which packets from outside are redirected should be left to the Fuss Server (if you want reachability of the same from remote). Therefore, another IP in the internal network should be used.

For an example, please refer to the discussion in 1. of *Installing Proxmox on Debian*

8.3.3 3. Adjustment of repositories

Direct installation of Proxmox configures in `/etc/apt/sources.list.d/pve-enterprise.list` the "enterprise" repository which requires a subscription to their support agreement. We do not need this therefore you can delete this file, or comment out its contents (just append a `#` to the one line it contains).

It will then be necessary to add the "community" repository by running the command:

```
echo "deb http://download.proxmox.com/debian stretch pve-no-subscription" \
   > /etc/apt/sources.list.d/pve-install-repo.list
```

and then add the key that signs the repository packages by running the command:

```
wget -O- "http://download.proxmox.com/debian/proxmox-ve-release-5.x.gpg" | apt-key␣
↪add -
```

and, since the installer image generally does not contain the updates, run the commands:

```
apt-get update
apt-get dist-upgrade
```

and wait for the updates to install; if the kernel is among them, it will be necessary to reboot the machine.

8.4 Installation of fuss-server on Proxmox

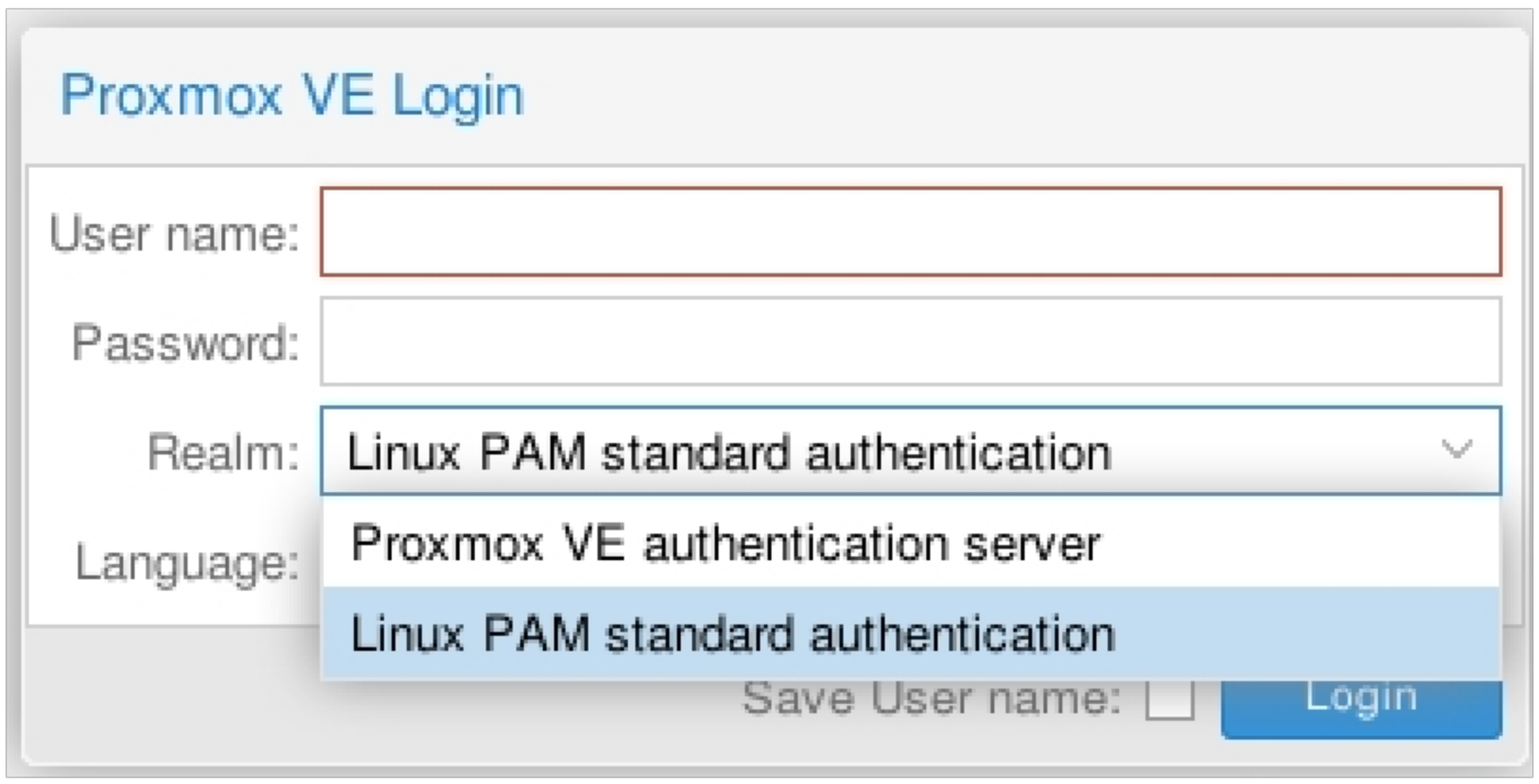
This page details all the steps you need to take to install Fuss Server on Proxmox, which are independent of the way the latter is installed, whether you did it with the installer, or whether you did it by first installing Debian and then switching to Proxmox.

8.4.1 General directions on connecting to the web interface

Every time you need to do an operation from the web-based management interface of Proxmox you will have to connect to the address:

https://IP.DEL.MIO.SERVER:8006

and you will get a login window like the following:



must be selected as "Realm" from the "Linux PAM standard authentication" menu, and you will be able to connect using the credentials of the `root` user, entering `root` in the "Username" field and the corresponding password in the "Password" field.

Once authenticated, the following warning window for no subscription will appear, to which you can give OK without any problem.



8.4.2 Additional preliminary configurations

These are configurations to be made and checked after installation.

Synchronization of date and time

On Proxmox 4.4 time synchronization is performed by `systemd-timesyncd`, the configuration of which is maintained in `/etc/systemd/timesyncd.conf`, which by default is empty so the NTP servers in the Debian pool are used.

If the machine has access to the Internet, no further action is required, otherwise the file will need to be modified to indicate which NTP server to address (e.g., an NTP server on the internal network, which could be provided by the router, for example).

In such a case, it will be necessary to include content such as:

```
[Time]
Servers=IP.DEL.SERVER.NTP
```

Alternatively, you can directly install the NTP service on the machine with:

```
apt-get install ntp
```

Again for proper synchronization you need to set up access to a reference NTP server, to do this you must:

- open the `ntp` configuration file (`/etc/ntp.conf`) for example with `vim /etc/ntp.conf`
- Comment out existing server entries and add the IP address of the server you can reach to synchronize date and time

An example of the content that can be changed is as follows:

```
server  0.debian.pool.ntp.org  iburst
server        1.debian.pool.ntp.org
iburst                        server
2.debian.pool.ntp.org  iburst  server
3.debian.pool.ntp.org iburst
```

If the default synchronization with `systemd-timesyncd` is not working you must intervene manually. The following commands can be executed to verify that the clock is synchronized (and at the same time verify that the indicated NTP server is reachable):

```
service ntp stop
ntpdate tempo.ien.it
# synchronize clock to hw clock
hwclock         --
systohc   service
ntp start date
```

Creating bridges for interfaces

In the Proxmox installation (or the Debian installation) only the first network interface is configured. Fuss Server uses at least a second one for the local network (we will assume it is `eth1`) and possibly a third for the captive portal (we will assume it is `eth2`). The installation leaves them unconfigured and we will assume this as a starting point.

In order to use them from the virtual machines, a corresponding bridge must be configured (it will be `vmbr1` and `vmbr2`, respectively. To do this, connect to the web interface, and access the network configuration section with the following actions:

- Click on the Node (e.g., "server102") in the first panel
- Click on "Network" in the second panel

At this point press on the "Create" button and from the menu select "Linux Bridge", a configuration window will be proposed in which the only field that needs to be set is "Bridge ports" in which to enter the name of the relevant

interface (e.g. for `vmbr1` you would put `eth1` for the internal network, for `vmbr2` you would put `eth2` for the captive portal).

In the case of the configuration of the captive portal interface, it is not appropriate to configure an address, but an additional specific configuration of the Ethernet interface dedicated to it turned out to be necessary in order to avoid upload slowdowns that occur with some interfaces. For this reason, it is necessary to disable in the network in- terface the "generic segmentation offload" and "TCP segmentation offload" features. This is done manually with the command:

```
ethtool -K eth2 gso off gro off tso off
```

continuing to assume that the interface dedicated to the Captive Portal is `eth2`; note that the configuration applies to the interface, not the bridge. To make the configuration permanent, the command can be set up by adding under `/etc/network/if-up.d/` a `cp-iface` script to execute it, with content like:

```
#!/bin/sh

# disable GRO, GSO and TSO from captive portal interface,
# to avoid upload slowdown

ETHTOOL=/sbin/ethtool

test -x $ETHTOOL || exit 0

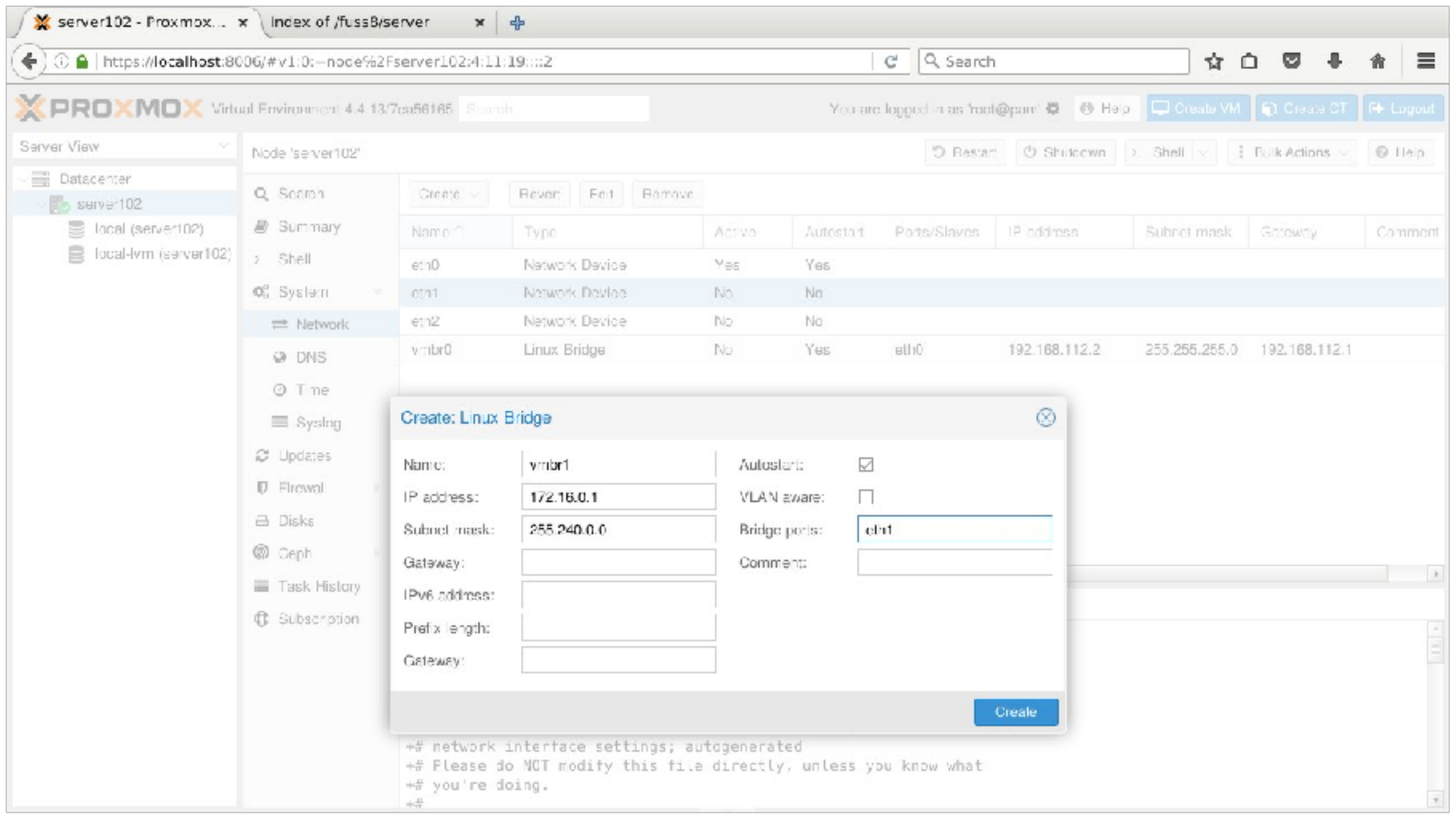
[ "$IFACE" != "eth2" ] || exit 0

$ETHTOOL -K eth2 gso off gro off tso off
```

For the configuration of the internal network interface if you want to reach the Proxmox machine from it you will need to give an IP address to the bridge as well, taking care to enter it outside the range that you will later use for the DHCP of the Fuss Server (and obviously different from the one we will assign to the Fuss Server itself). In that case the fields to be filled in are:

- IP address : put the desired address
- Subnet mask : put the subnet mask that you will use on the internal network
- Gateway : must be left blank
- Bridge ports : put eth1

An example is shown in the figure; the configuration is finalized by pressing "Create."



To apply the new network configuration, the machine must be restarted (this can be done directly using the "Restart" button on the web interface).

8.4.3 Upload ISO images to the server for virtual machine installation

Uploading can be done through a direct download to the server (e.g., with `wget`) or by di- rectly copying the file to the `/var/lib/vz/template/iso` directory. Files in this directory must be ISO images of the installation CD/DVD.

In the case of the Fuss Server, the most up-to-date one that can be downloaded from the

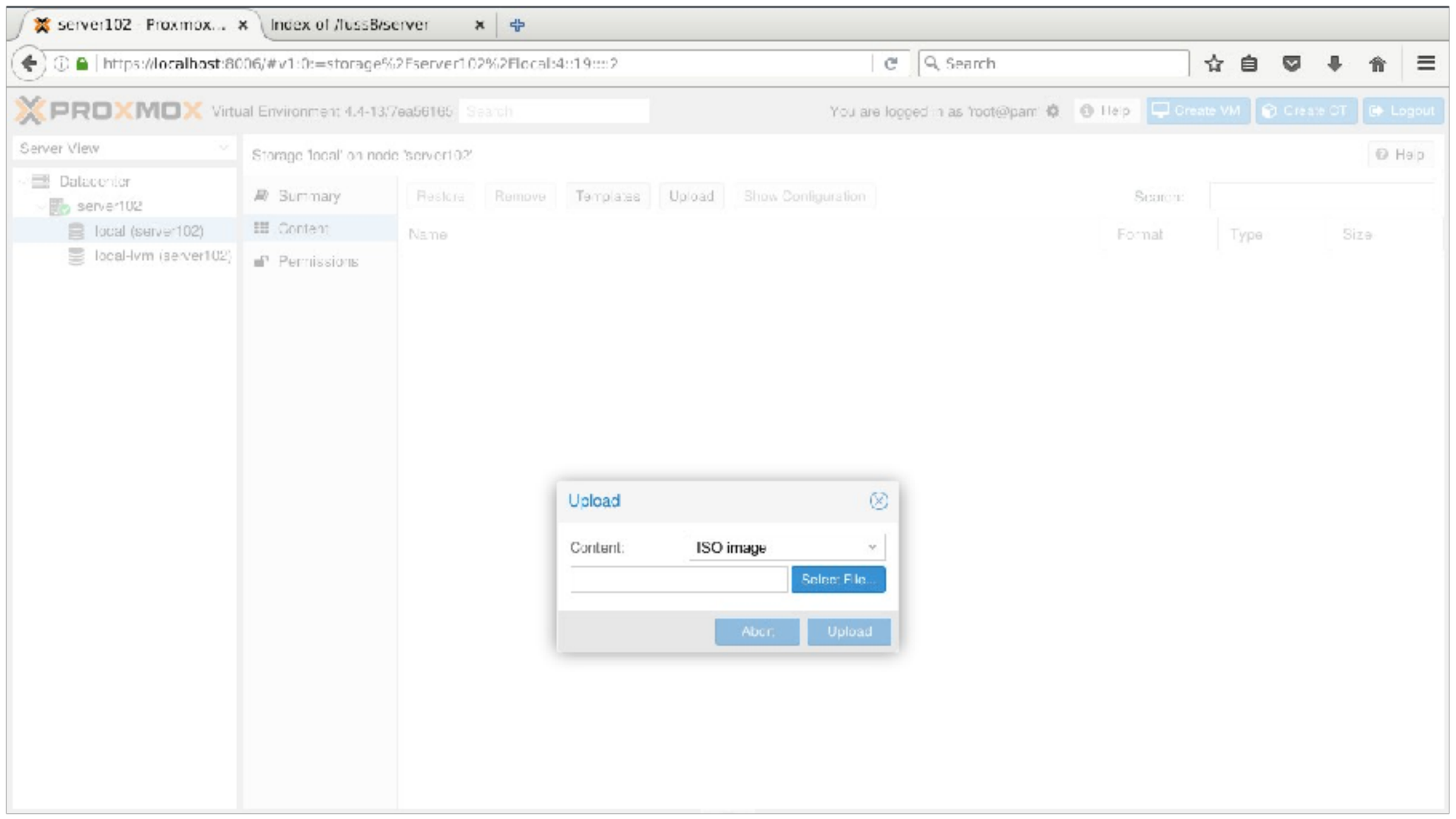
following address should be used: http://iso2.fuss.bz.it/fuss8/server/

(e.g. "fuss-server-jessie-amd64-201705221525.iso")

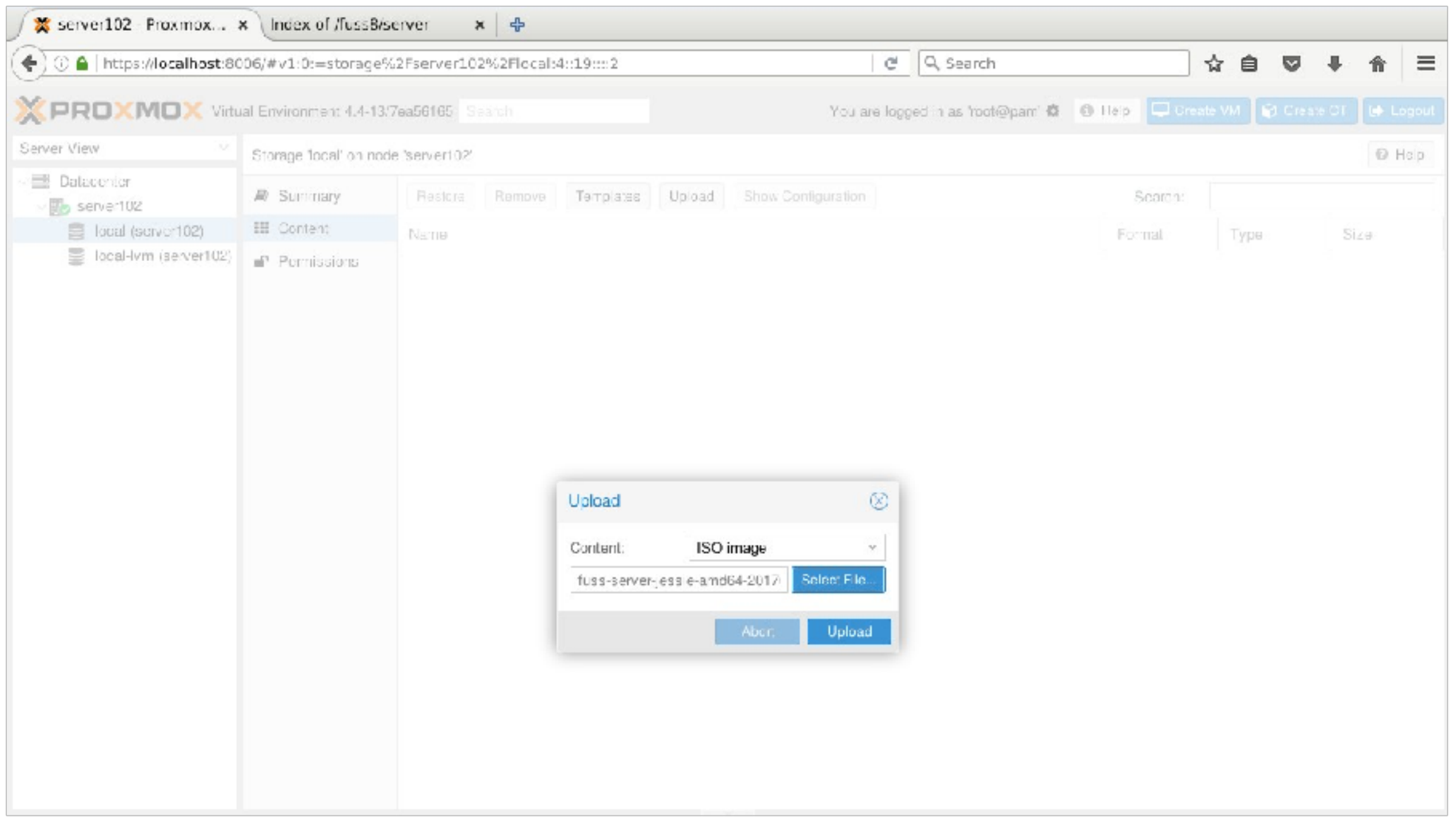
Should you have the image on your PC, you can upload it directly from the web interface, to "local" storage. To do this you perform the following steps:

- from the left menu, click on "local (server)"
- from the side menu select "Content"
- from the central menu, click on

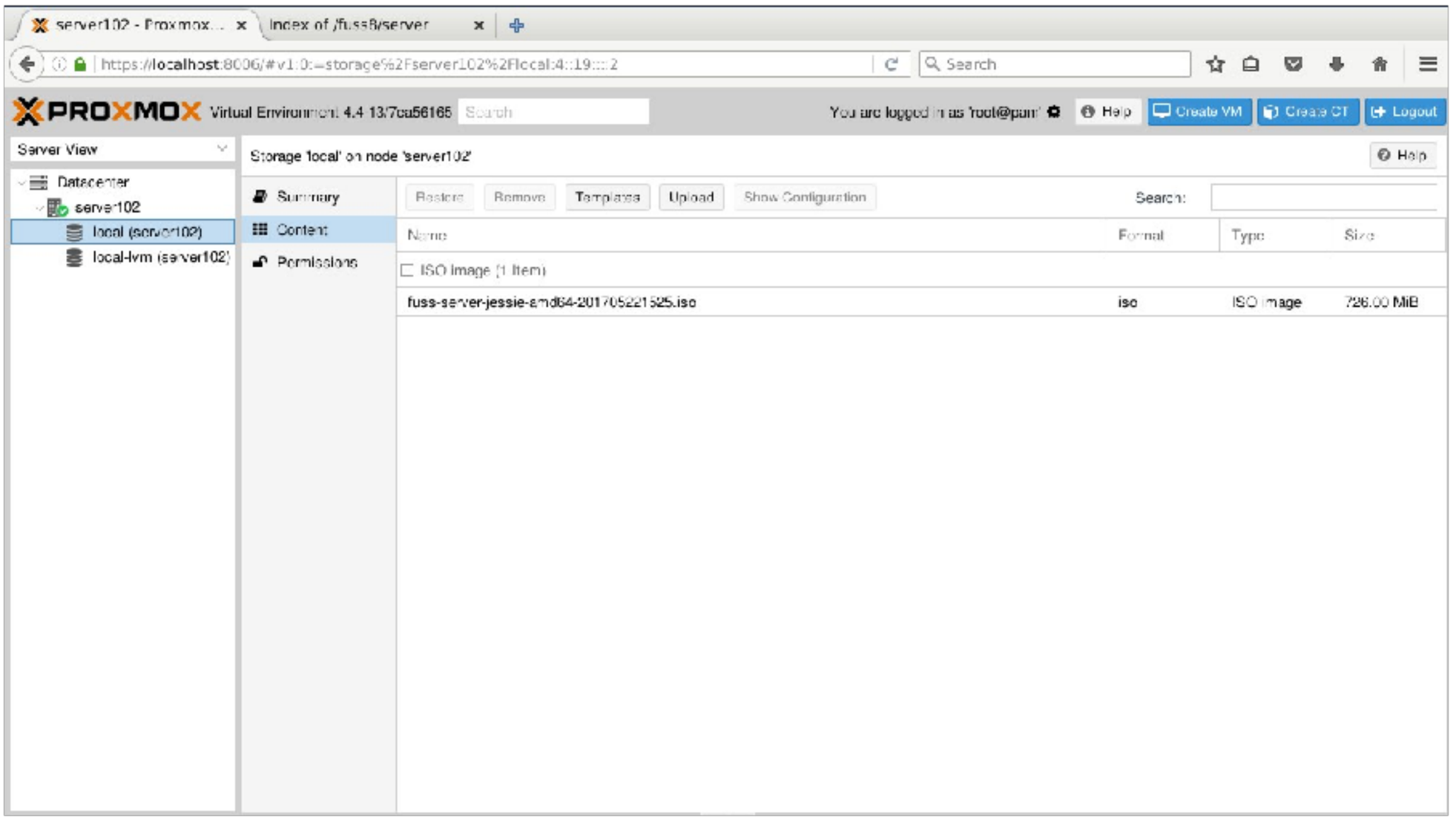
"Upload" you will get the following screen:



at this point click "Select file" and choose the downloaded ISO (you can also load it directly from an external device) and once selected you will get:



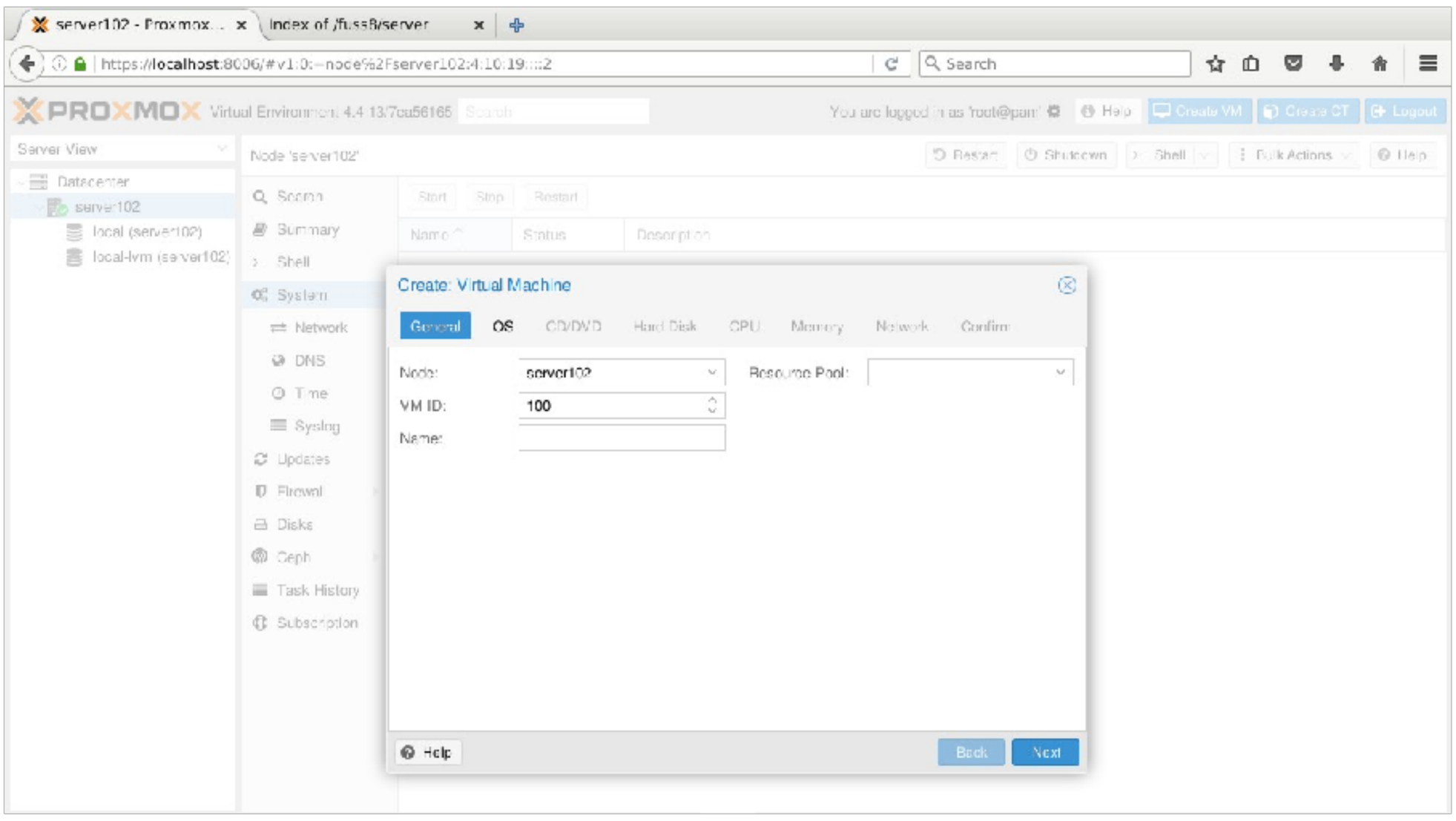
at this point you will be able to click on "Upload," when the upload is finished, you will see the uploaded ISO as in the figure:



8.4.4 Creating the virtual machine for the Fuss Server

Virtual machine creation procedure

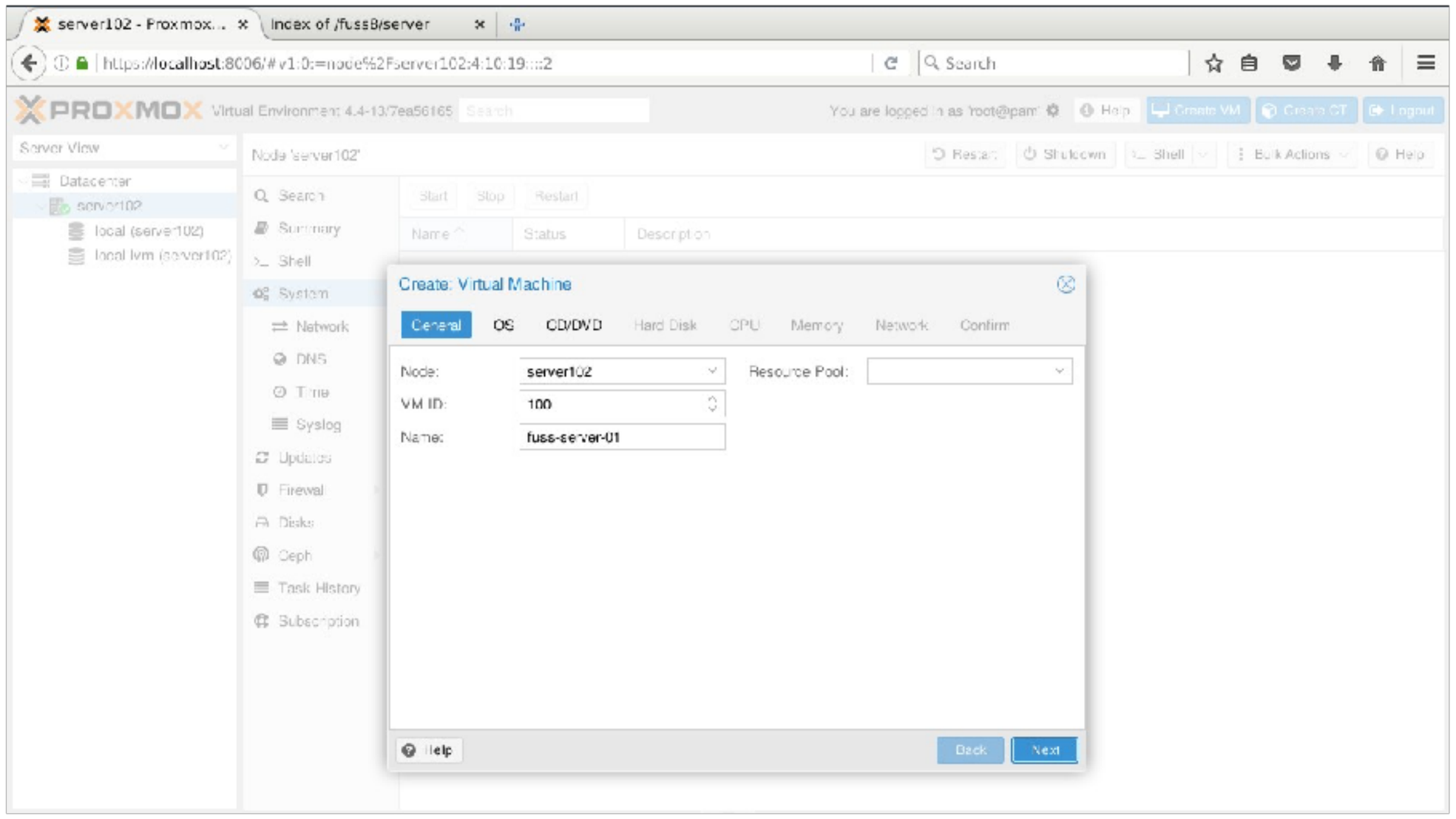
Creation is triggered by clicking on the light blue "Create VM" button in the upper left corner, which will bring up a window like the one in the figure:



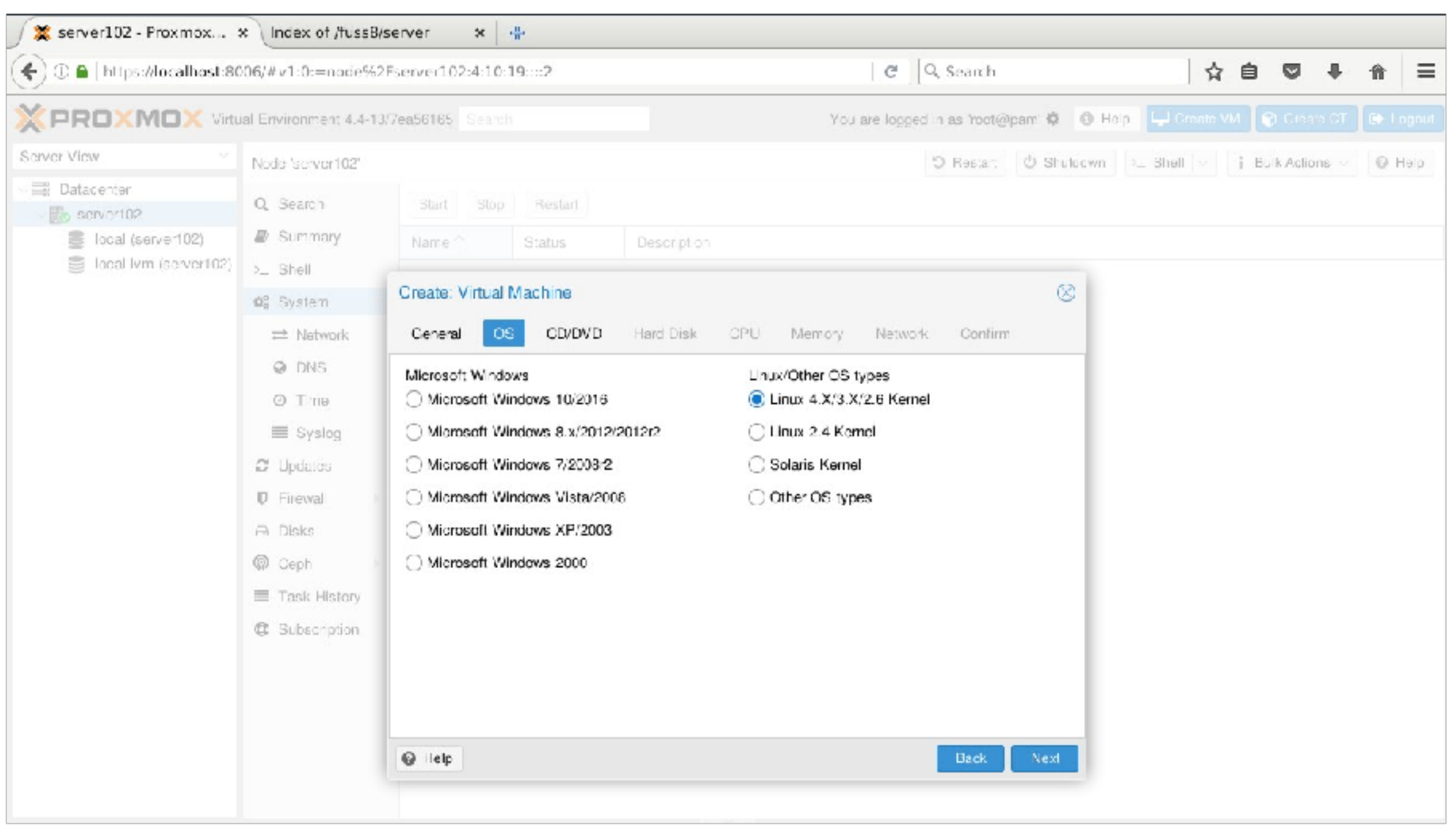
which involves making a series of value settings divided into sections, following a succession of screens navigable back and forth with the "Next" and "Back" buttons, and identified by a label at the top.

1. Section: "General," enter only
    - VM ID: (you can accept the default, 100)

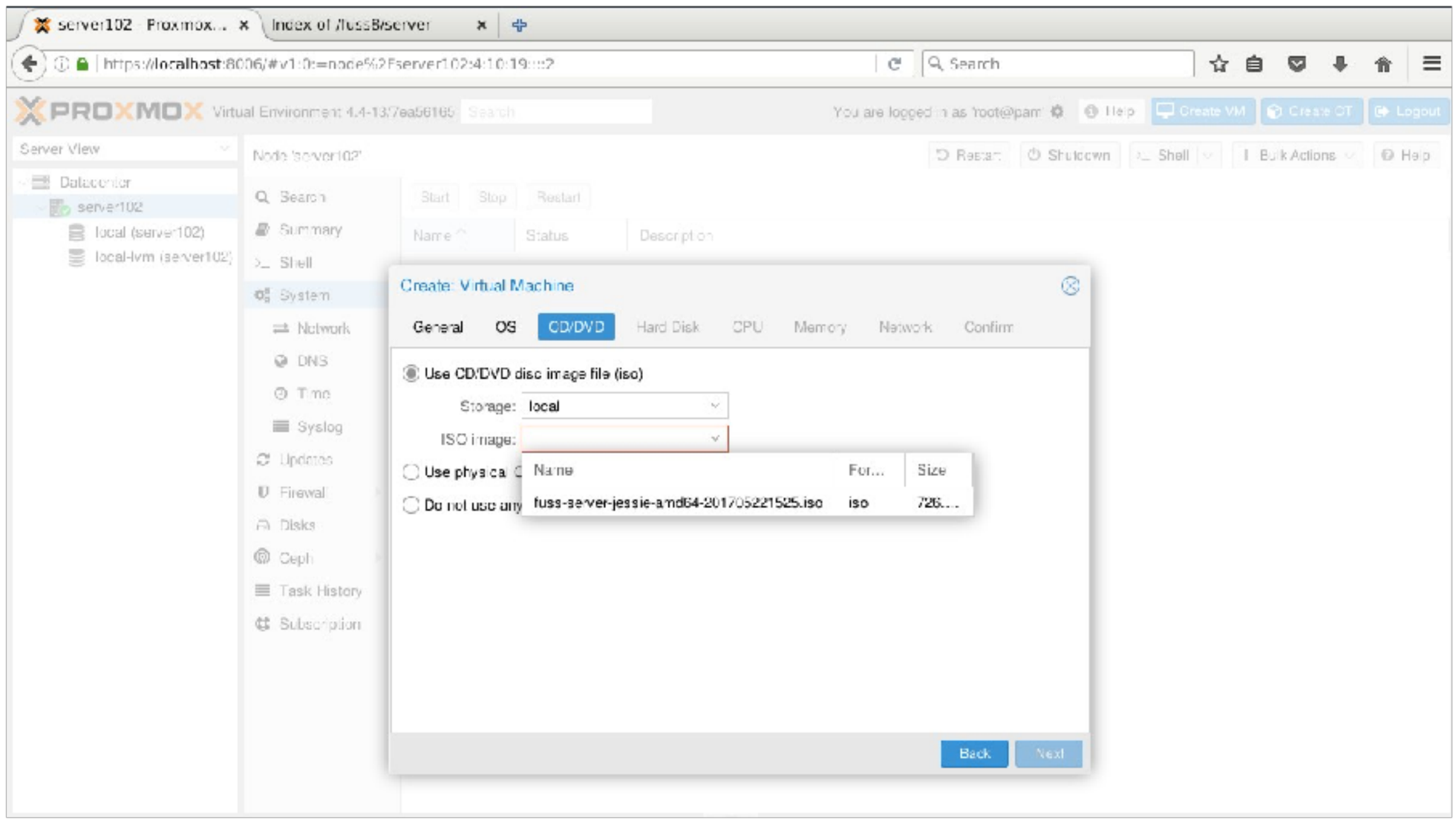
- Name: an identifying name (e.g. fuss-server-01; the same name as fuss-server is recommended)



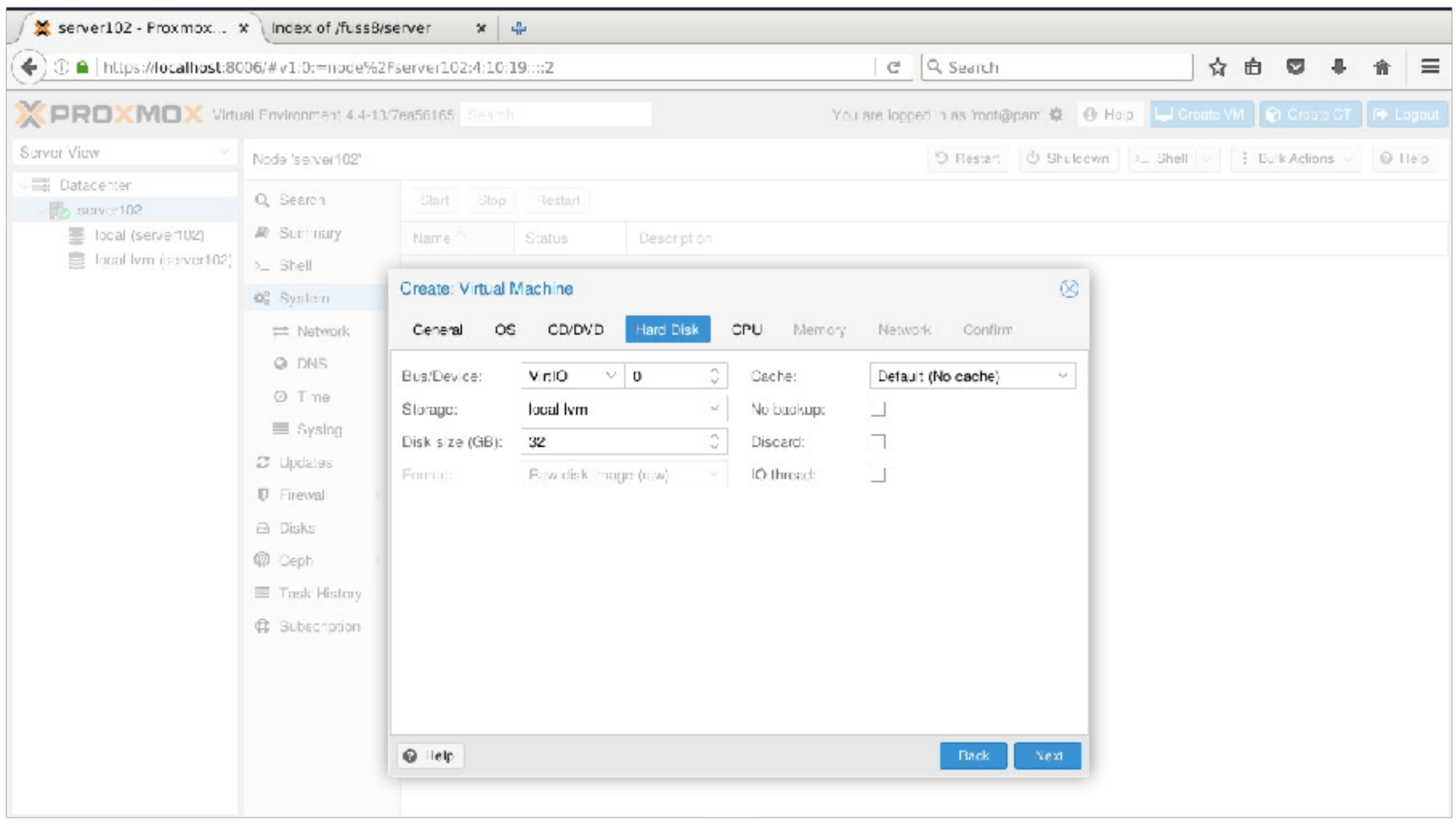
2. Section: "OS"
   - select "Linux 4.X/3.X/2.6 Kernel"



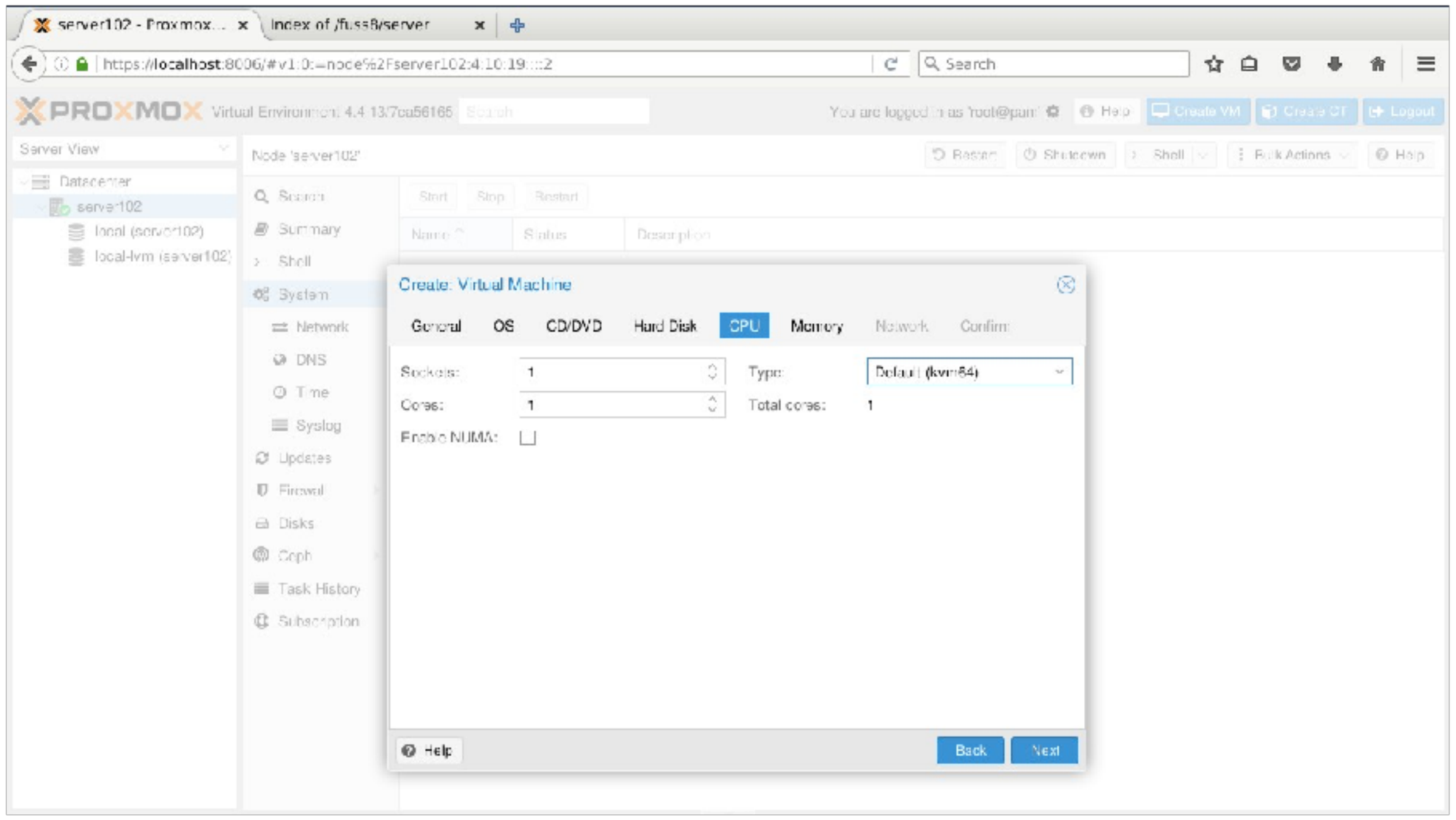
3. Section: "CD/DVD"
   - expand "ISO image:" dropdown
   - Select the previously loaded ISO (for example: "fuss-server-jessie-amd64-201705221525.iso")



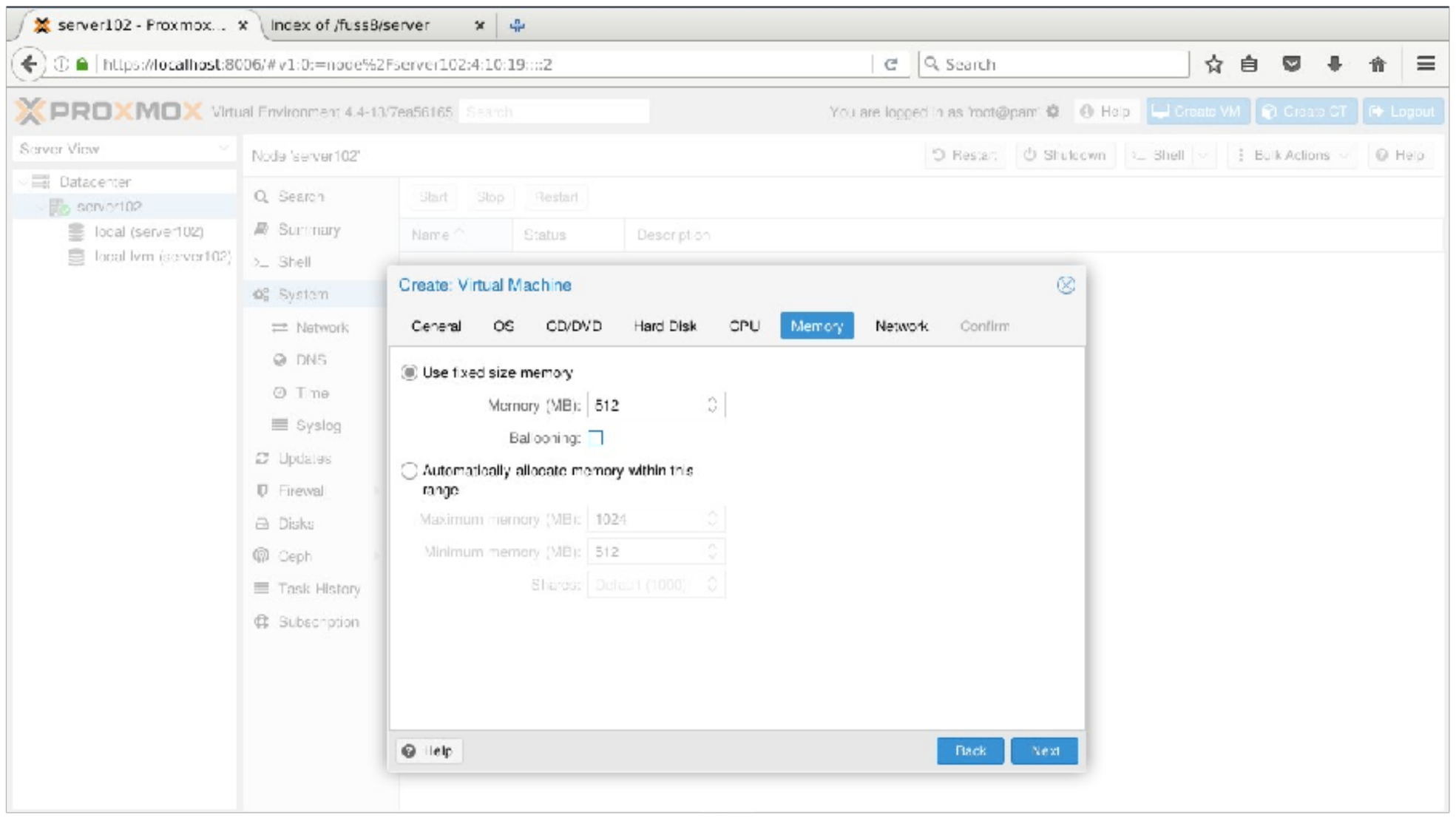
4. Section: "Hard Disk"
    - Bus/Device = VirtIO
    - Storage = local-lvm
    - Disk size (GB)= size of disk in GB, see instructions in 4.2
    - Format = Raw disk image (raw) (NOT MODIFiable)
    - Cache = Default (No cache)



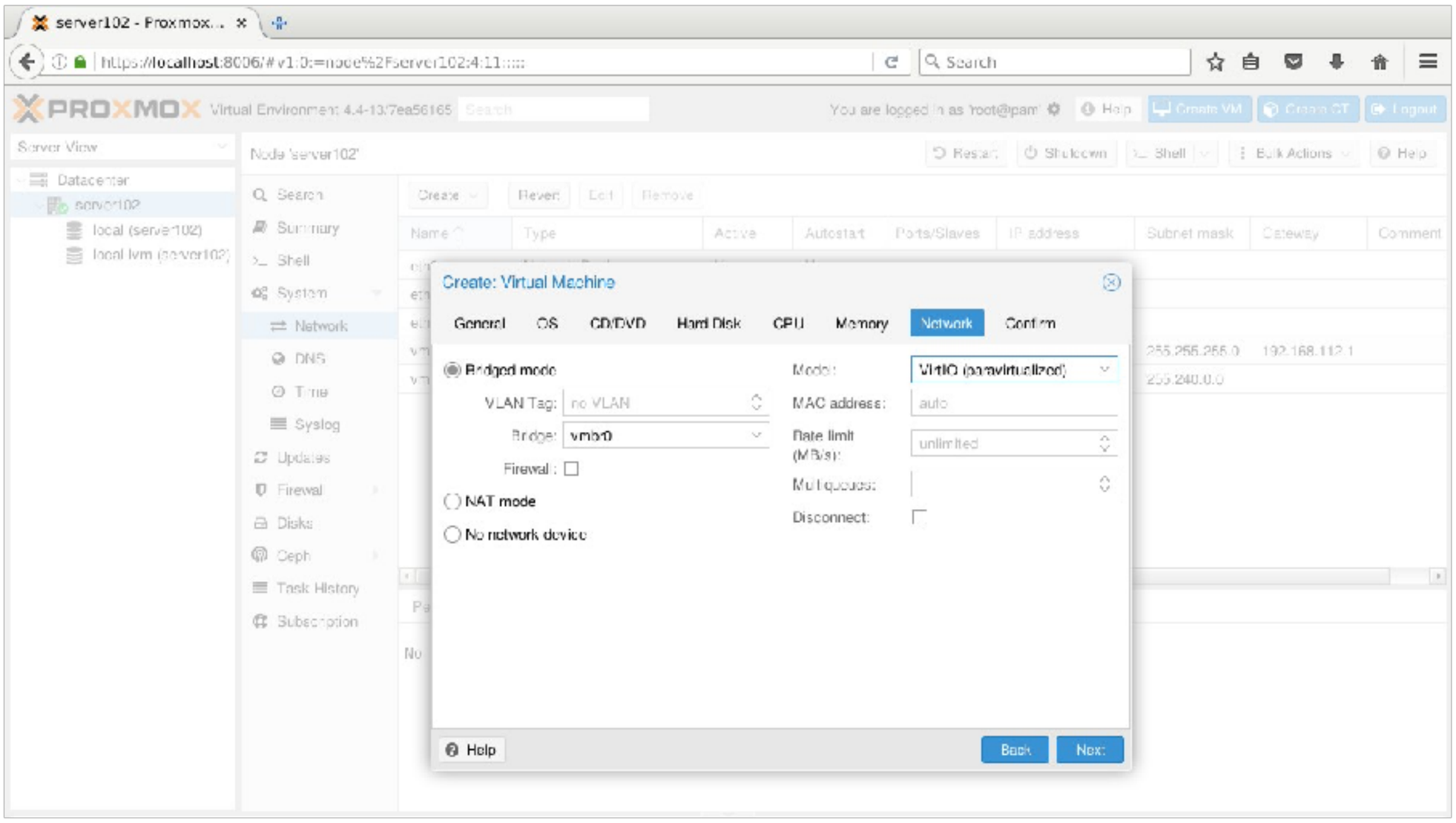
5. Section: "CPU"
    - Socket: equal to the number of processors in the machine, see instructions in section 4.2
    - Cores: 1



6. Section: "Memory"
    - Memory (MB) : RAM of the machine, choose according to the directions in section 4.2
    - Remove the "flag" to the "Ballooning" function.



7. Section: "Network"
    - Bridge = vmbr0
    - Model = VirtIO (paravirtualized)



Sizing for RAM, CPU and disk

For memory sizing, the Proxmox developers suggest leaving at least 1G of the machine's total RAM for the system, you can allocate the remainder for virtual machines, for the fuss-server the actual needs may vary depending on the number of users who will use it.

The choice of the amount of RAM also depends on whether the physical machine will be used to host other virtual machines. A good starting choice is to employ one-half to three-quarters of the total, leaving a lung of resources to increase RAM later (just change the value from the web interface and restart the machine).

For CPU sizing, we check the number of processors in the machine and state it as the number of cores (the use of sockets and cores is indifferent for performance, the total product of the two values counts; the possibility of varying them is in favor of those who have software licenses by number of sockets, which we do not care about).

Hint: To find out the number of processors in the machine you can use the `top` command, press 1 to view separate statistics by CPU and count the relative rows present.

For disk sizing, a total size assigned to virtual machines com- patible with the maximum size available on the disk space pool of the `given` logical volume must be chosen. The current situation is obtained with the `lvs` command; for example:

```
# lvs
  LV            VG  Attr                LSizePool Origin Data% Meta% Move Log
↪%Sync Convert
  data          pve twi-aotz--  514.06g             11,48  5,66
  local         pve -wi-ao--------200,00g
  root          pve -wi-ao----------20,00g
  swap              -wi-ao----    4,00g
  vm-101-disk-1 pve Vwi-aotz-- 100.00g data         59,04
```

In this example the size allocated to the pool (logical volume `data`) is 514.06 G, and virtual machine 101 has been allocated 100G. The space can be increased at will (from the interface), but to avoid the root possibility of running out of space on `data` never exceed an allocation equal to 95% of the pool size (logical volume `data`).

> **Warning:** the `Data%` and `Meta%` percentages refer to actual usage, which is certainly less than the theoretical maximum (in the case 100/514 ~ 20%). The use of the pool allows the so-called *overcommit*, i.e., allocating more disk space than is actually available, a situation to be avoided at all costs. In fact, allocating more disk space for virtual machines than is available, if this is later exhausted, results in disastrous data loss.

Therefore when creating the fuss-server, provided that no other virtual machines are planned to be created later, it will be sufficient to use a value less than 95% of the size (in the previous case 514.06g) available on `date`. Remember that reducing the excess disk space allocated to a machine at the beginning is always more complicated than extending it when it turns out to be little. If disk space is still available in the volume group (it will be if you left it during installation keeping a "lung" as recommended) it is still possible to enlarge `data` with the command:

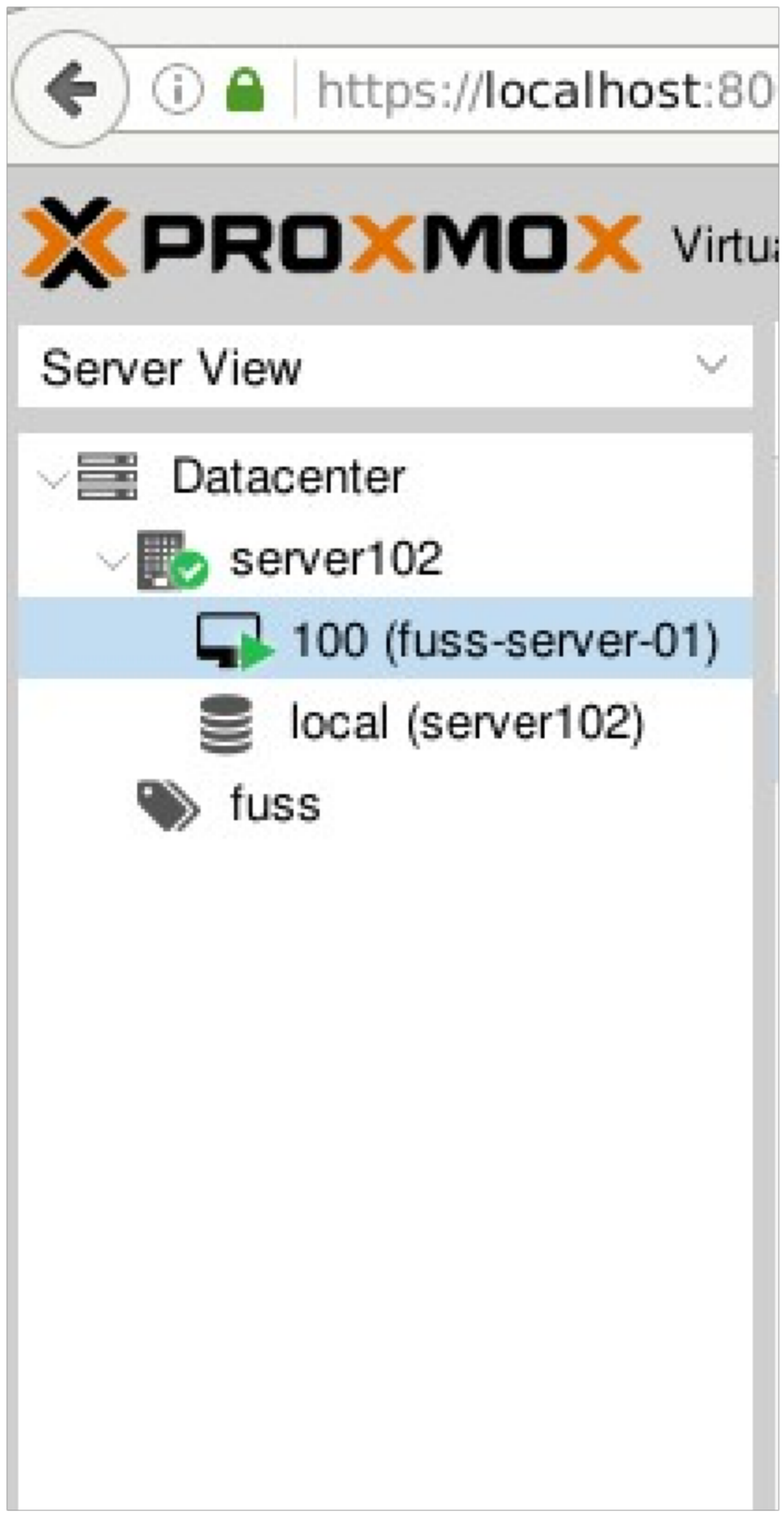
```
lvextend -L +XXg /dev/pve/data
```

and then possibly use the extra space obtained.

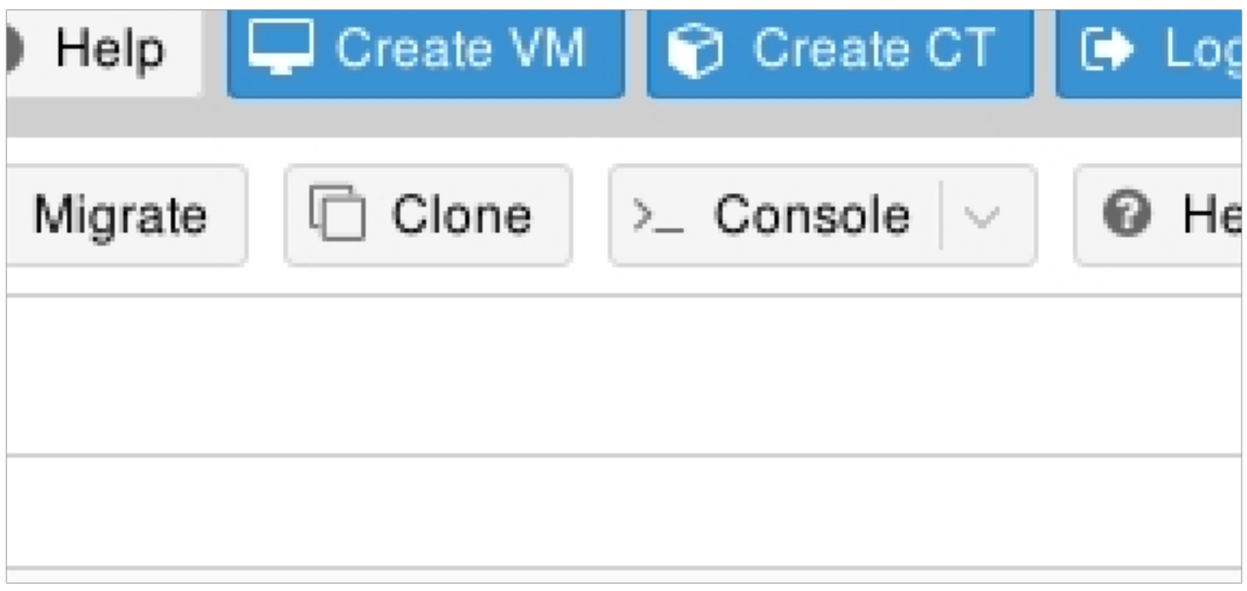
Start the virtual machine

Once you create the virtual machine, it will appear in the panel on the right, to start it, and at the same time have access to the console, you can follow the following steps:

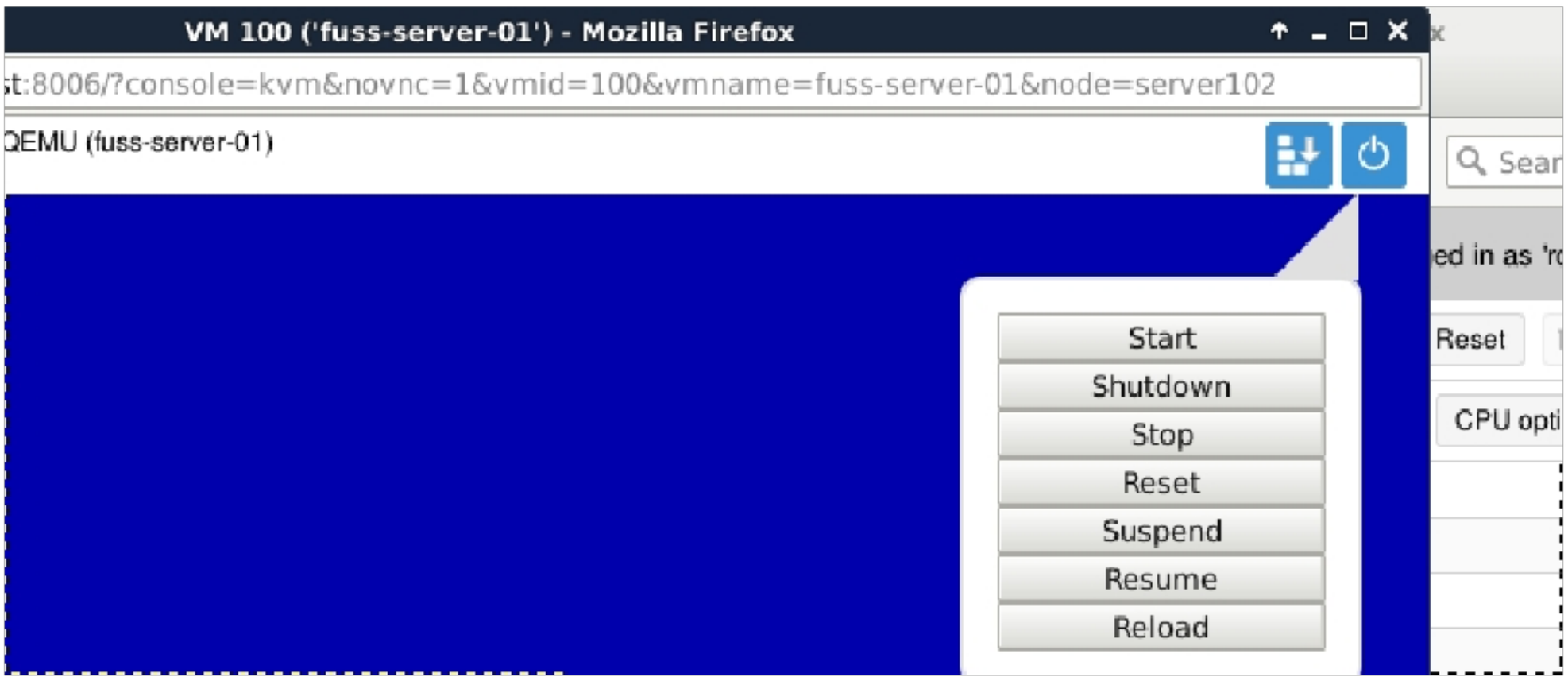
1. Select the VM, for example, "100(fuss-server-01)"



1. Select the "> Console" button in the upper right corner.

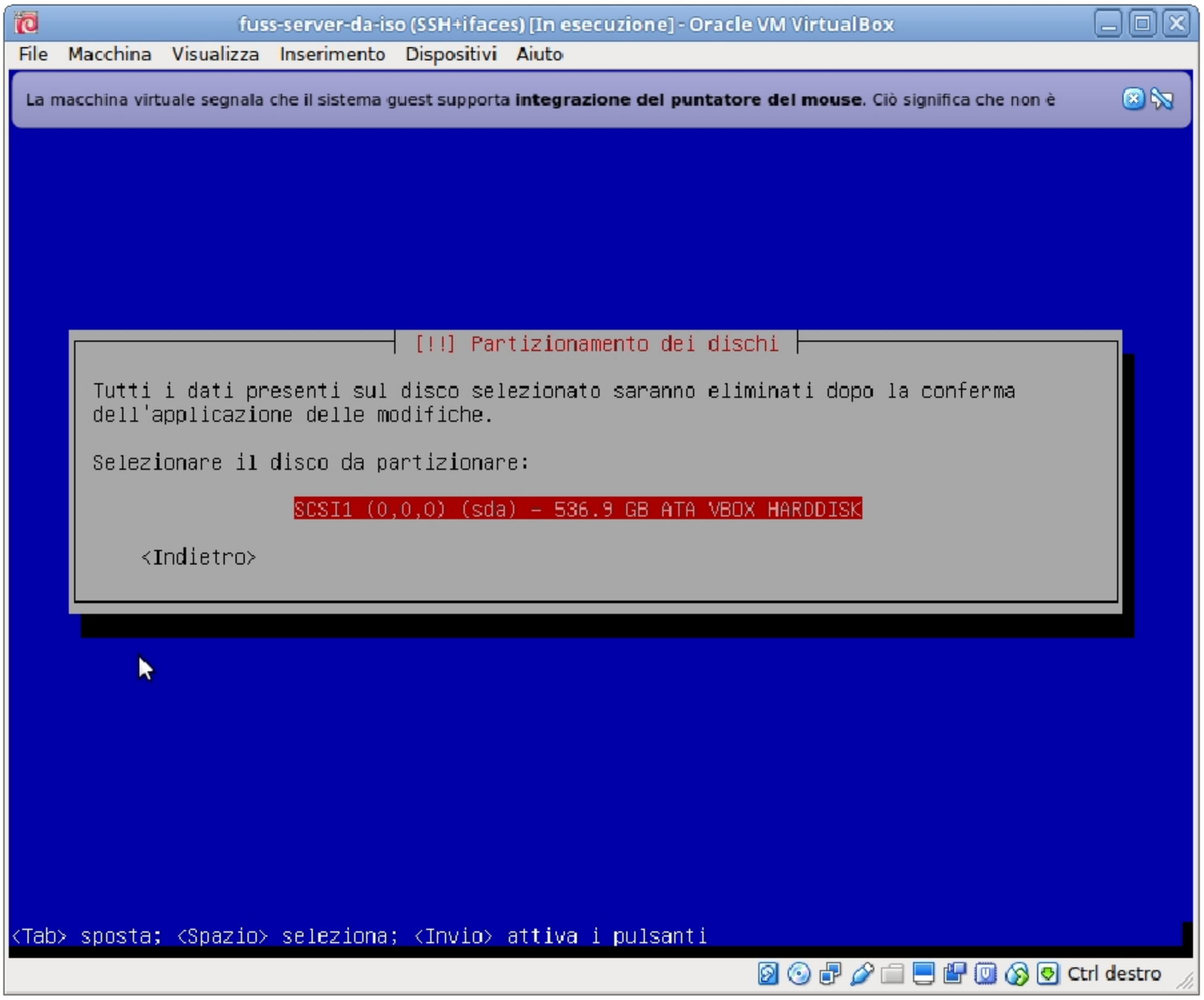


1. Choose "Start"

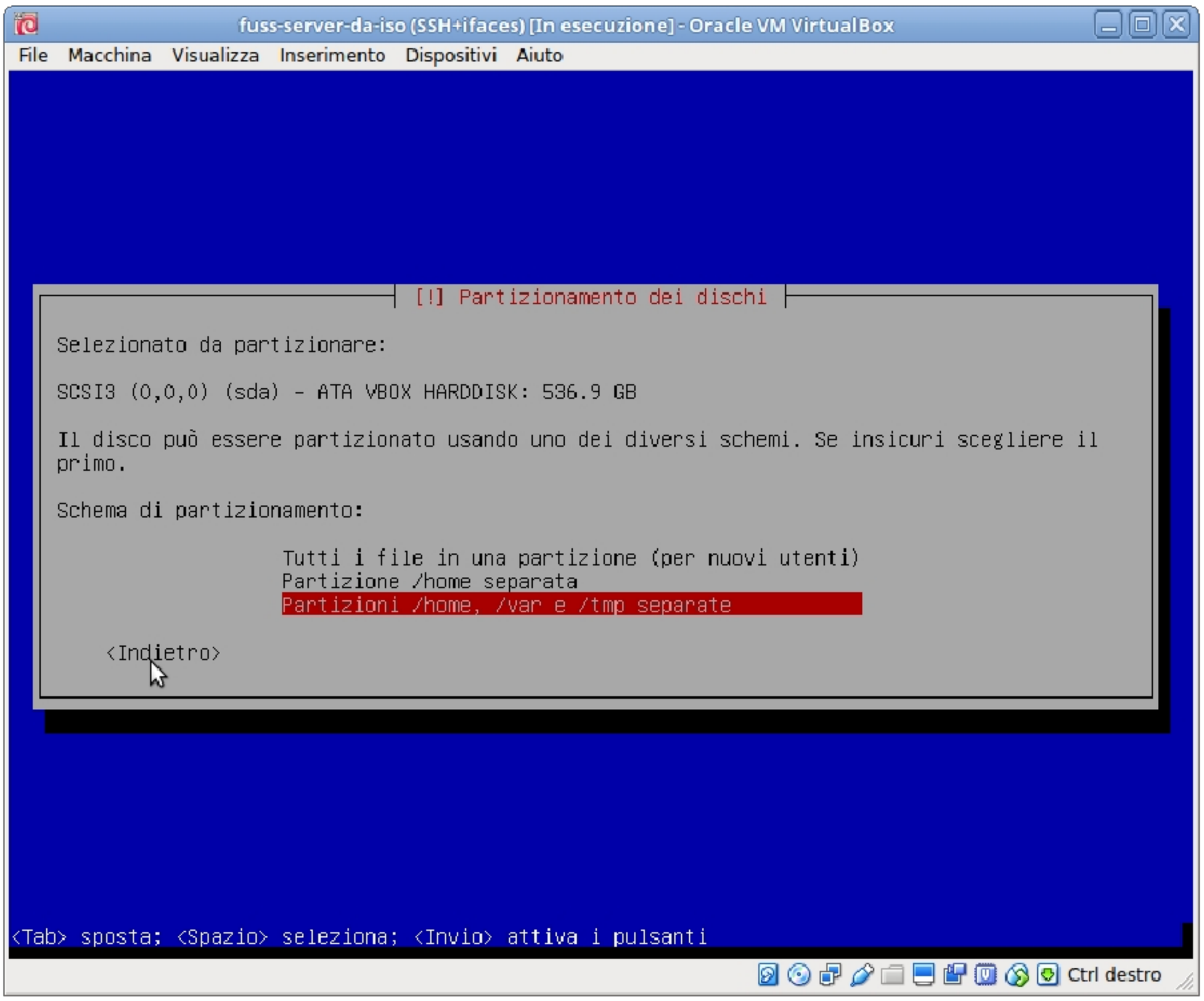


8.4.5 Installation of Fuss Server

Most of the fuss-server installation options are already preset in the ISO image, the only significant choice to be made during installation is the partitioning of the (virtual) disk assigned to it.

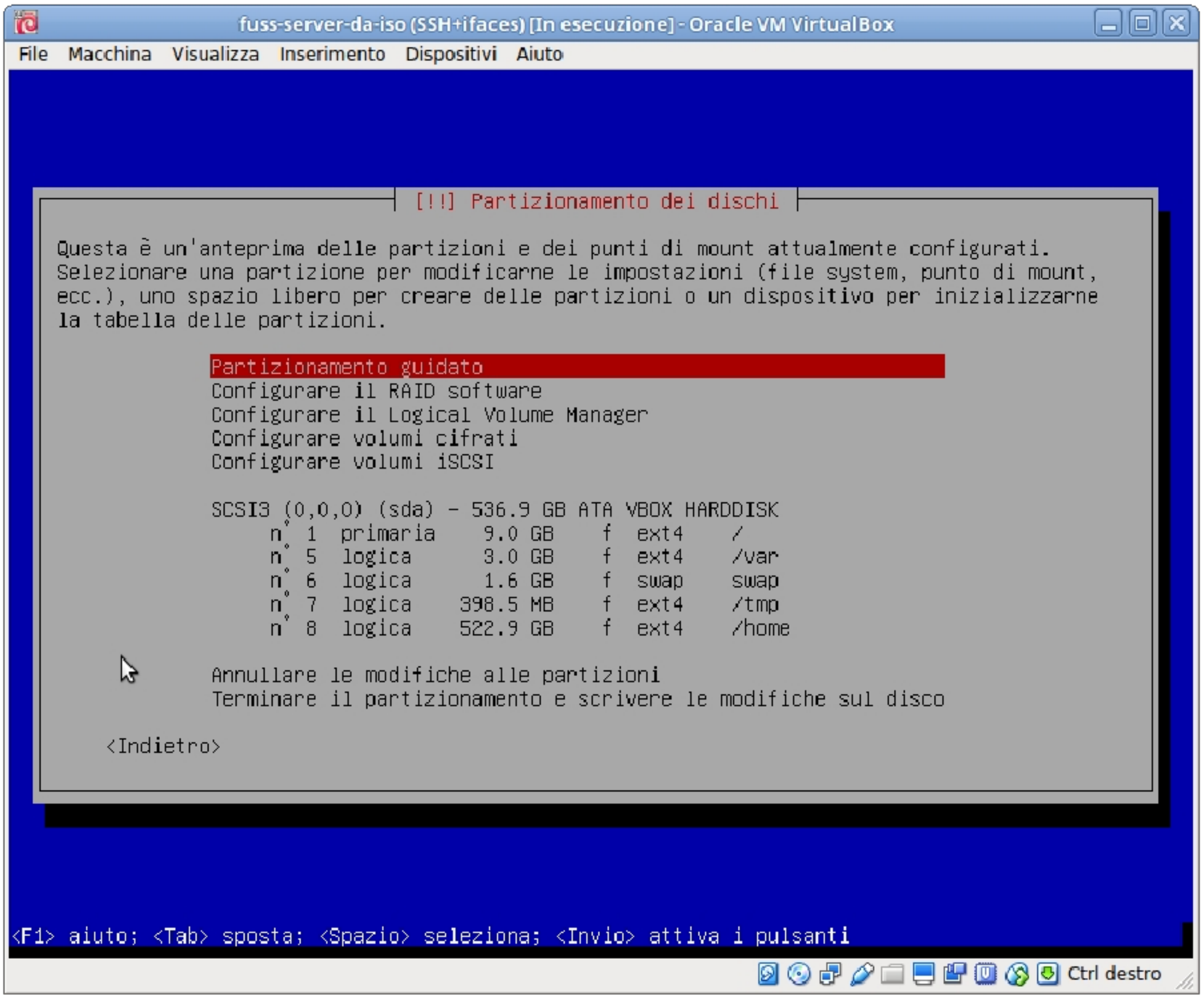


In the default choice after selecting the disk, its partitioning is proposed directly. The safest choice, to avoid root filling problems, is to use separate filesystems for `/home`, `/var`, `/tmp`. However, this with direct partitioning makes the eventual reallocation of disk space less flexible.

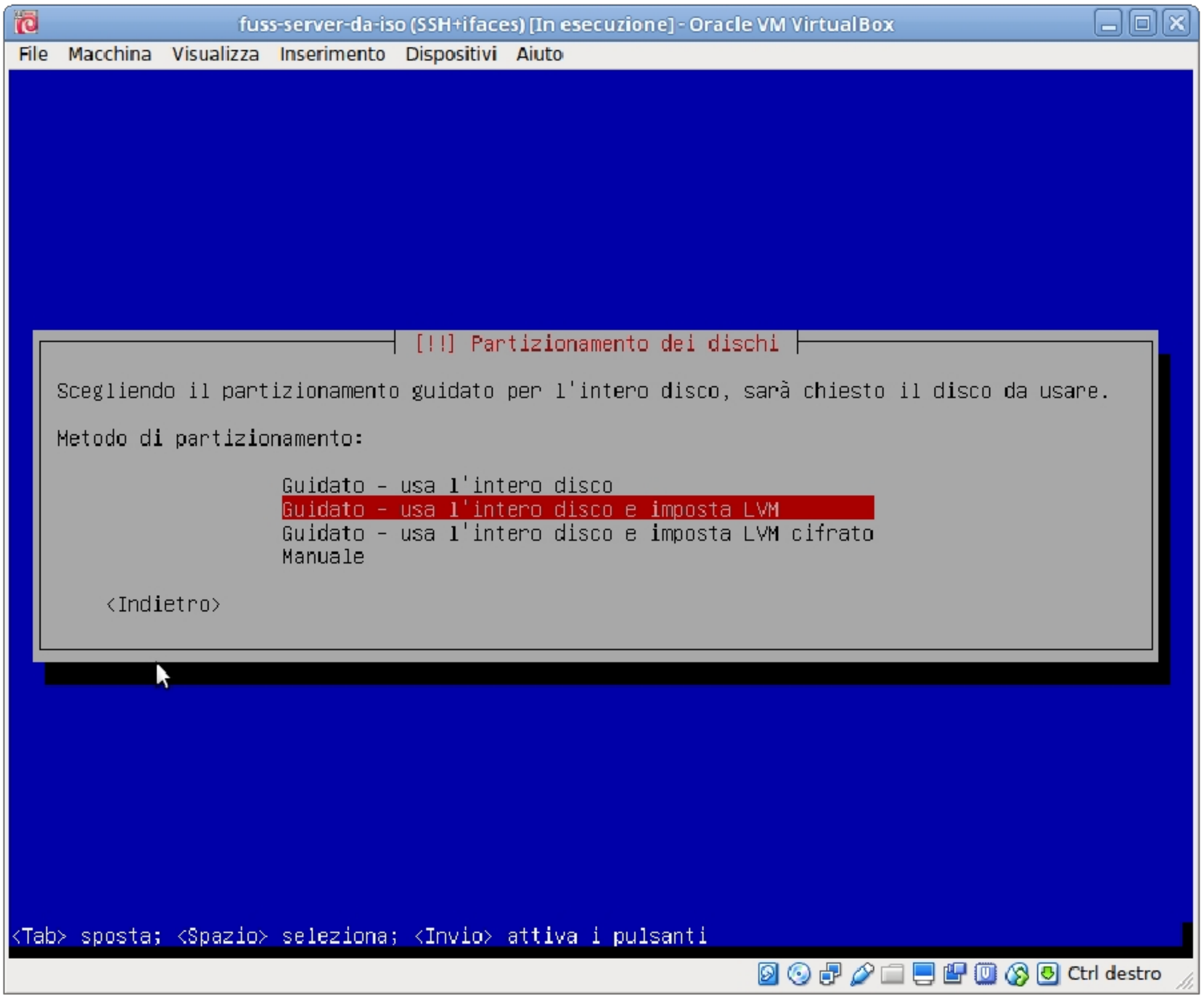


In fact, keep in mind that even if you have available disk space in the virtualizer to be able to enlarge the virtual machine disk, the enlargement would take place on the "bottom" therefore it would be easy to resize only the last partition (in the case of the `/home`, which while being the most likely one, is not necessarily really the one that needs the additional disk space).

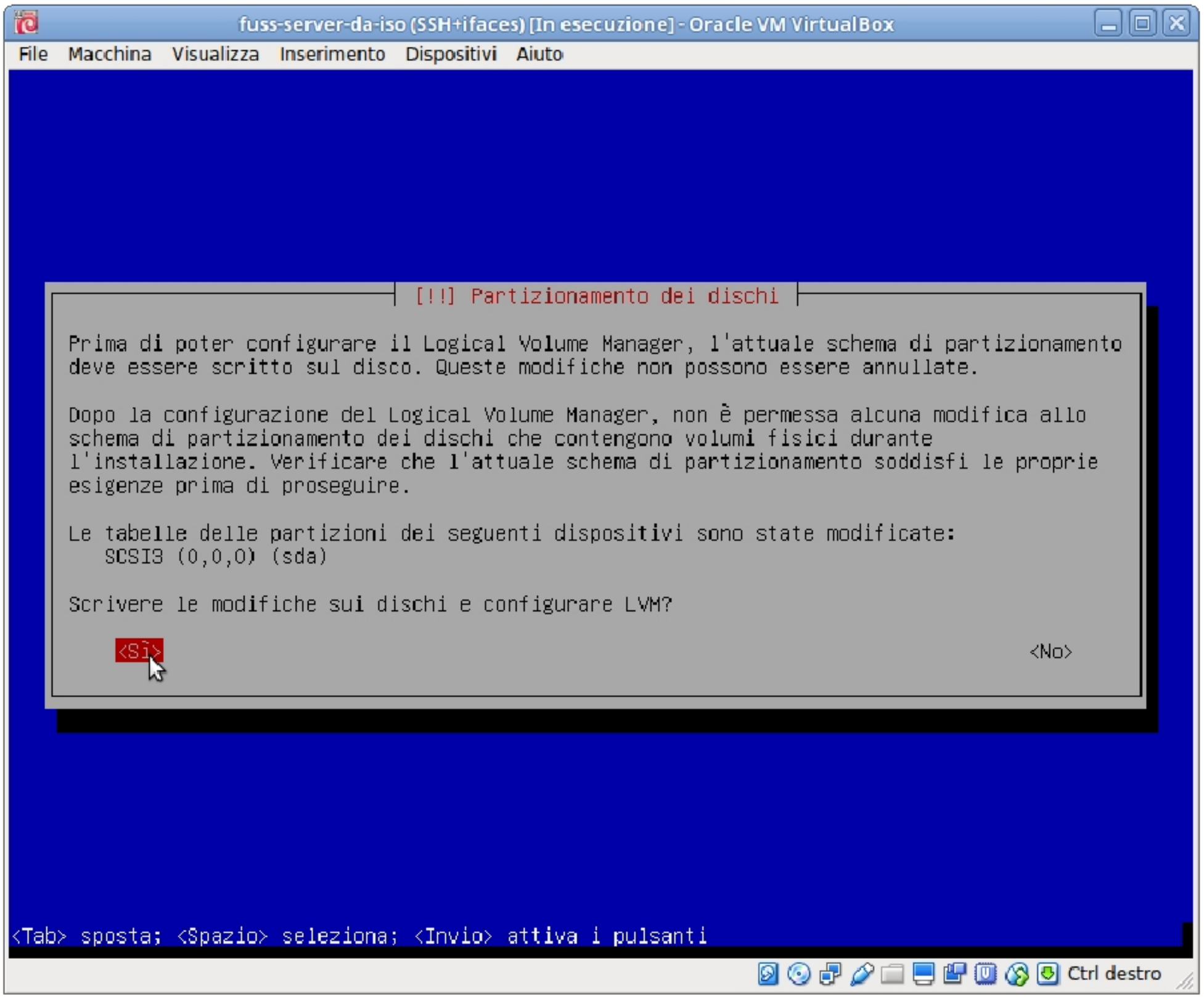
Therefore, it is suggested, for more flexibility, at the cost of a slight loss in I/O performance, to install using LVM. However, this means that once the previous choice is made, it will be necessary to "go back" by reselecting "guided partitioning."



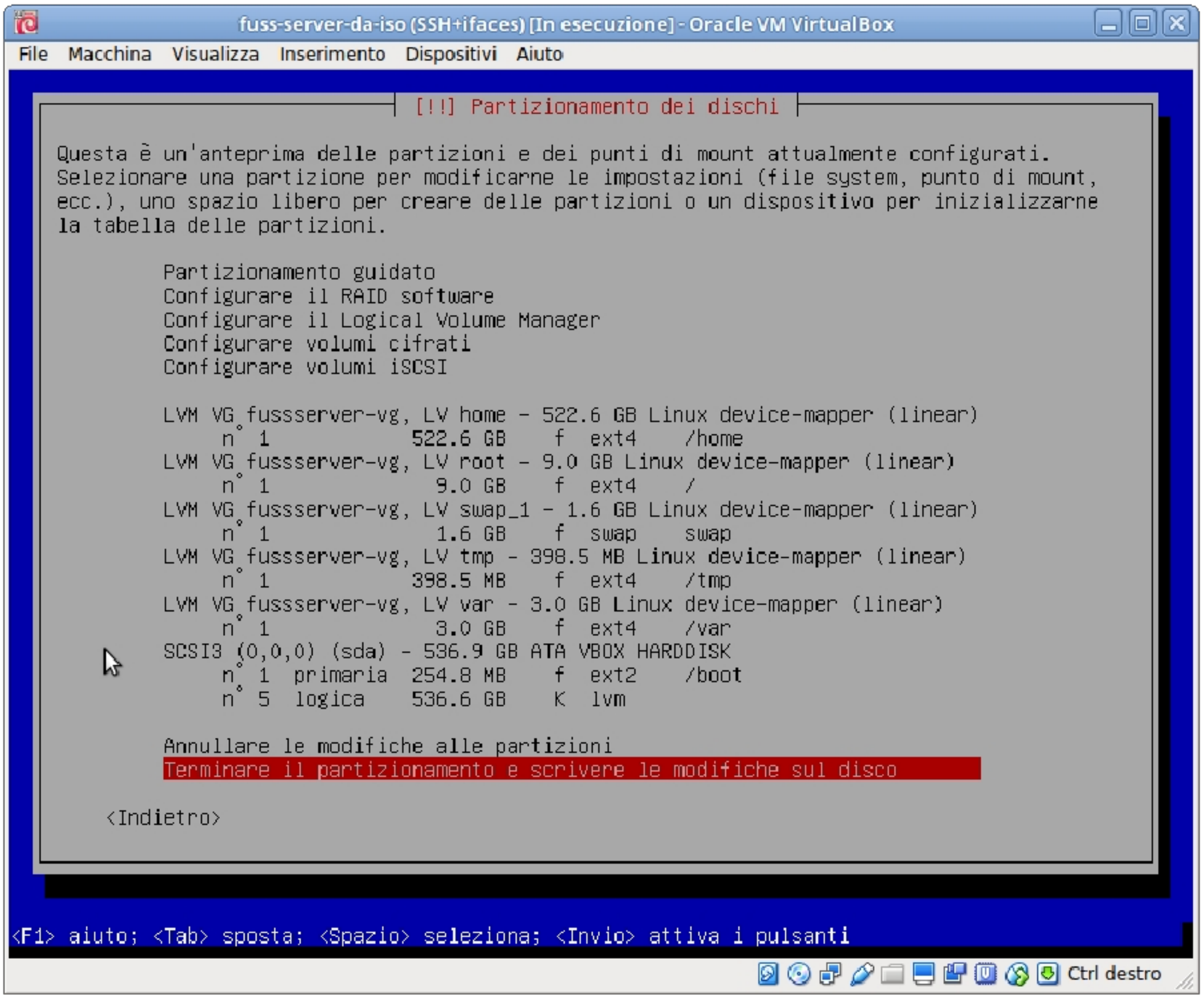
and then selecting "guided, use whole disk and set LVM."



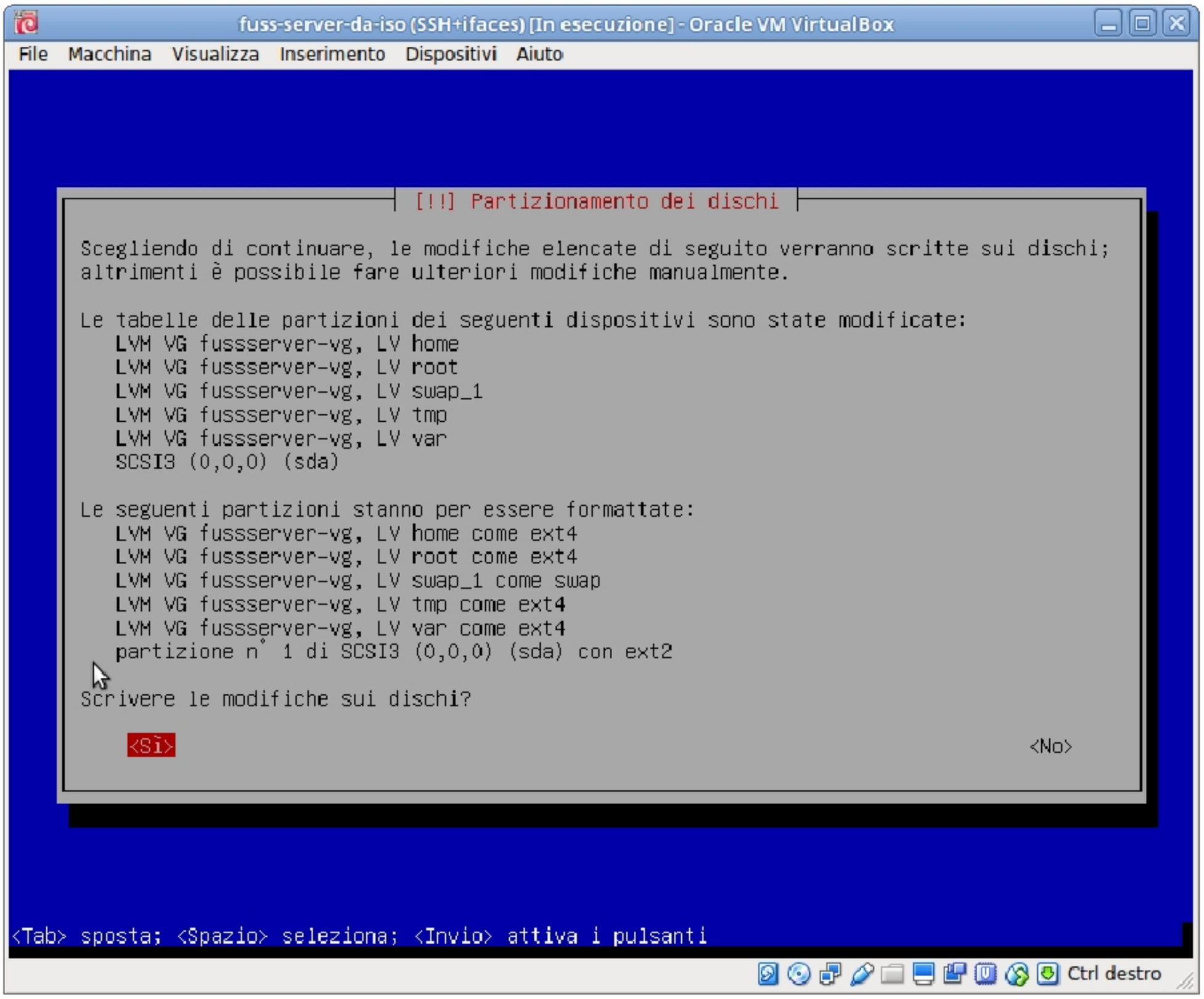
and at this point of will have to repeat the choice o f disk and use of separate filesystems, and confirm the LVM configuration:



and finally confirm the disk changes first:



And then the final formatting:



To this after any enlargement of the virtual machine disk, it will be sufficient to enlarge the final partition (which will be `/dev/vda5`, logical) that houses the LVM physical volume, extend the latter with `pvresize`, and then extend the filesystem you prefer with `resize2fs` (if you used the default of ext4).

8.4.6 Post-installation precautions of Proxmox.

Proxmox also provides its own firewall management system for the host for virtual machines, but the fuss-server already has its own internal firewall management, so the Proxmox firewall should not be enabled because it would interfere.

To protect the physical machine system, it is sufficient to install a simple firewall script that limits access from the internal network to ports 22 and 8006. In any case, this should not be visible directly from the Internet (the public IP address should be forwarded back to the fuss-server if necessary), so the need for a firewall is less compelling.

For machines that have hardware RAID controllers, it is suggested that some tools external to Debian be installed (check for licensing issues) to monitor their status. One site that contains several such programs, particularly for older and less supported controllers, is http://hwraid.le-vert.net/. It will still be necessary (the programs mentioned communicate via email) to define who will receive the relevant notifications.

It is also suggested to install some auxiliary control and utility packages such as:

```
apt-get tiger etckeeper debsums molly-guard atop iotop iftop
```

8.5 Machine cloning with clonezilla

The steps required to clone a machine on a whole lab are, on the machine to be cloned:

- *Start the first machine with Clonezilla*
- *Set up Clonezilla by selecting the server to be used for saving the image*
- *Clone machine*

And then on each of the other machines:

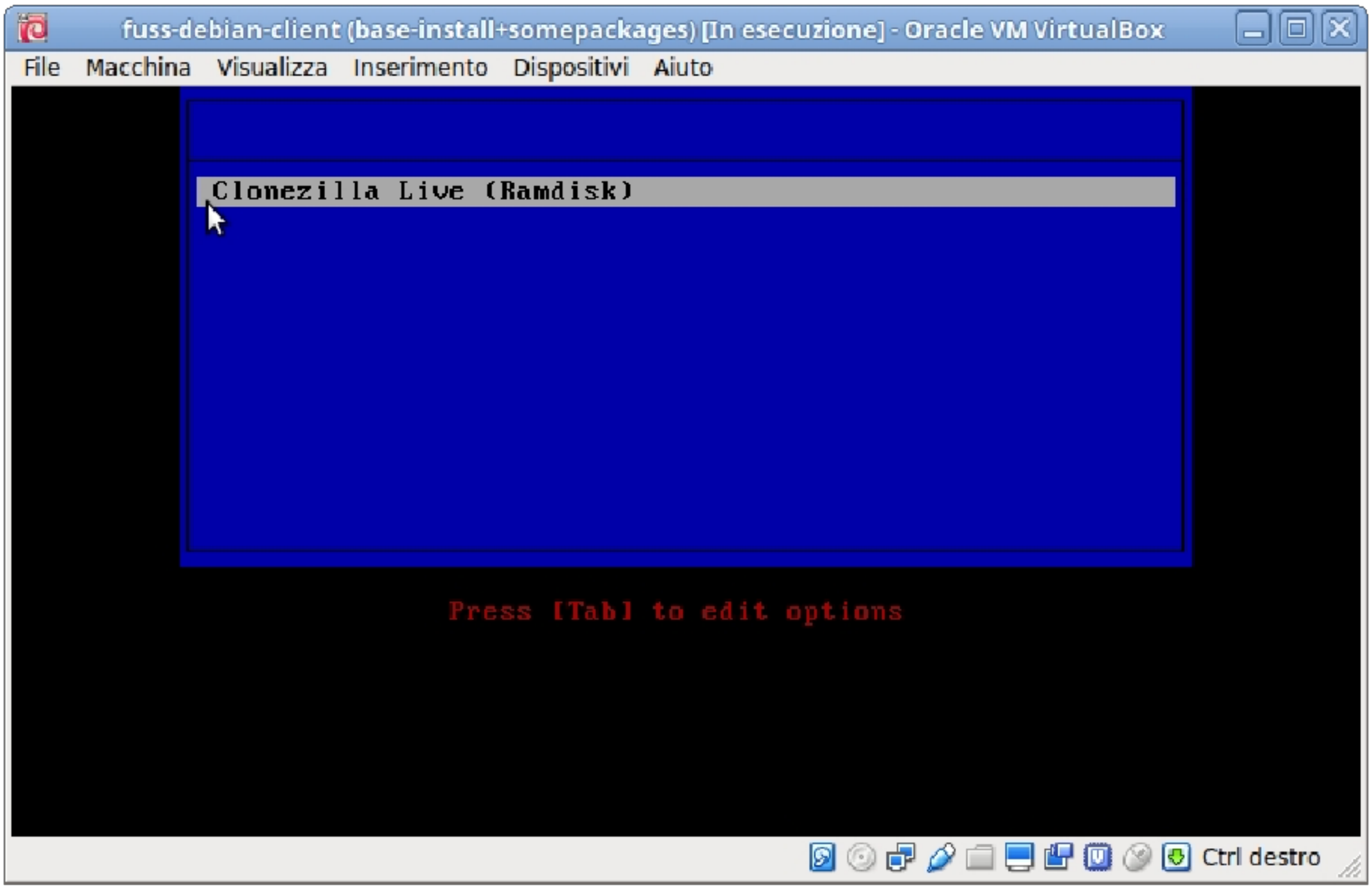
- *Start each of the other machines with Clonezilla*
- *Set up Clonezilla by selecting the server from which to obtain the image to restore*
- *Start the recovery procedure*

The images will be saved in the `/var/clonezilla` directory via ssh, using the `clonezilla` user with the password found on the server in `/root/clonezilla_cred.txt` (see *Manage clonezilla user/password*)

8.5.1 Clonezilla boot via network

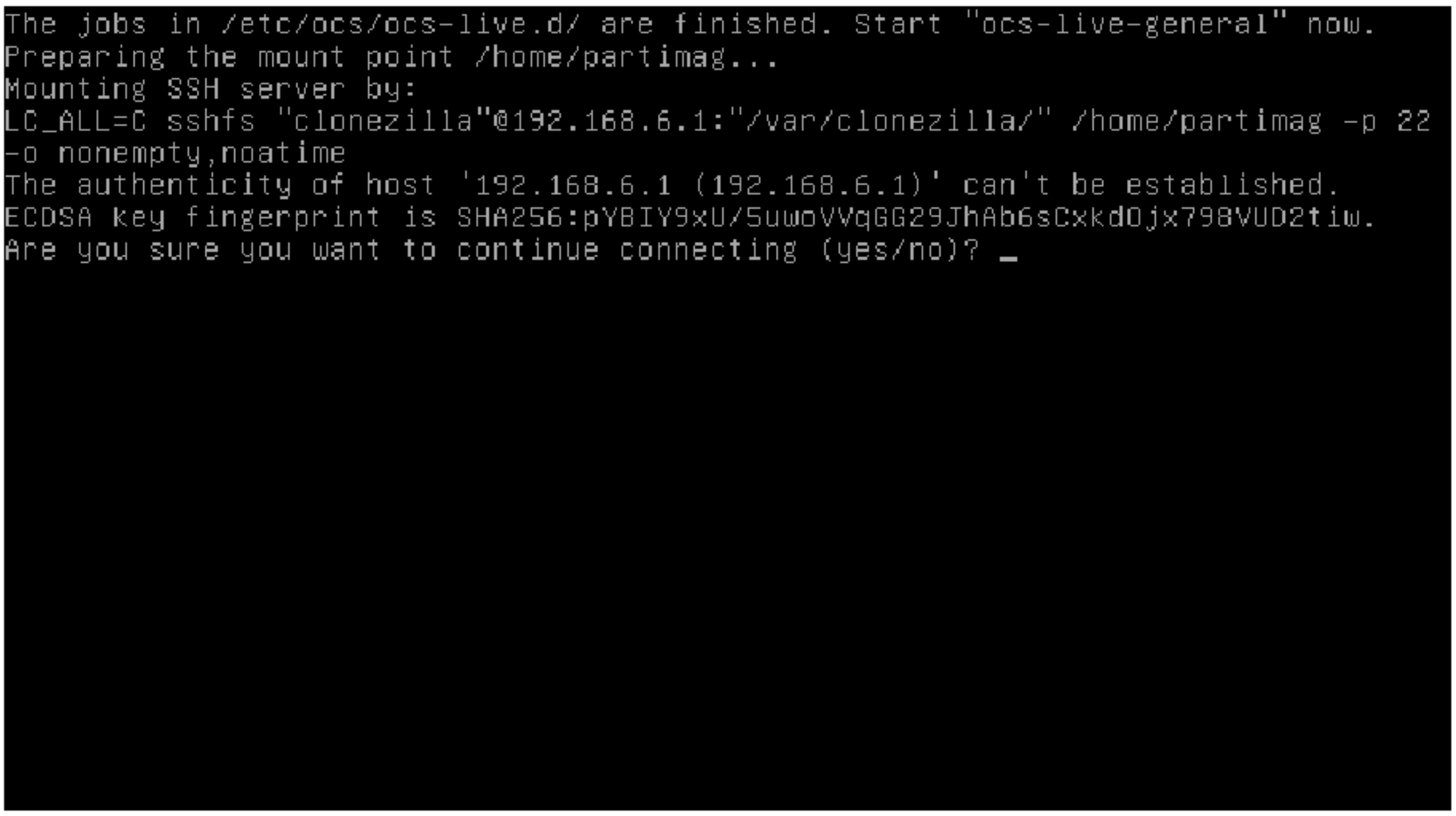
First, it is necessary to configure the various computers to boot from the network (PXE): how to do this depends on the different BIOSes on the computers, but generally it is enough to press a key to get the boot menu and select an item naming network, netboot, or PXE.

Then you will get the menu with the images available on the FUSS server: choose Clonezilla Live:

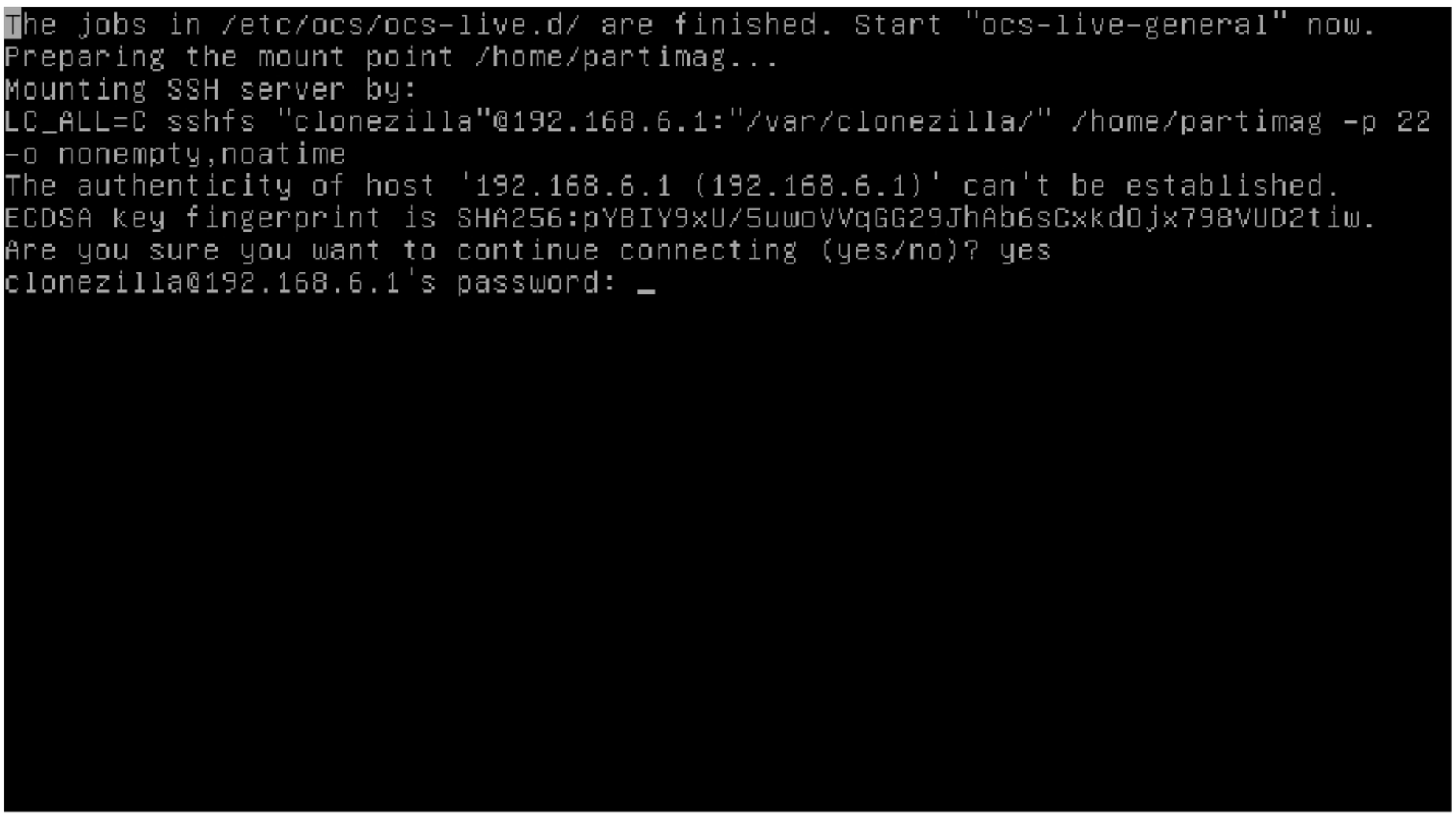


8.5.2 Configuring Clonezilla

You will first be asked to confirm the server fingerprint (being on a local network you can safely accept it):



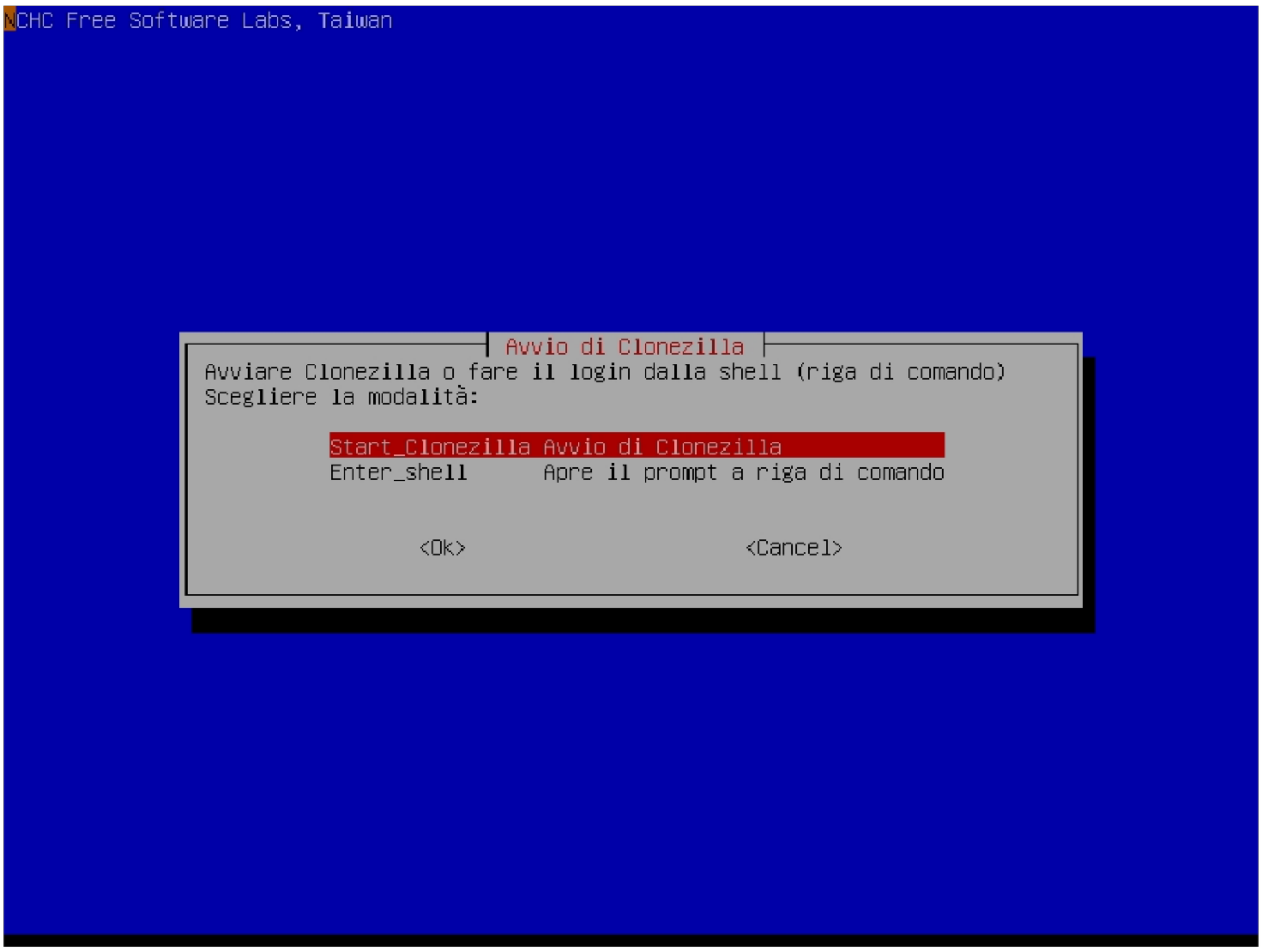
then enter the clonezilla user's password, found in the `/root/clonezilla_cred.txt` file on the server:



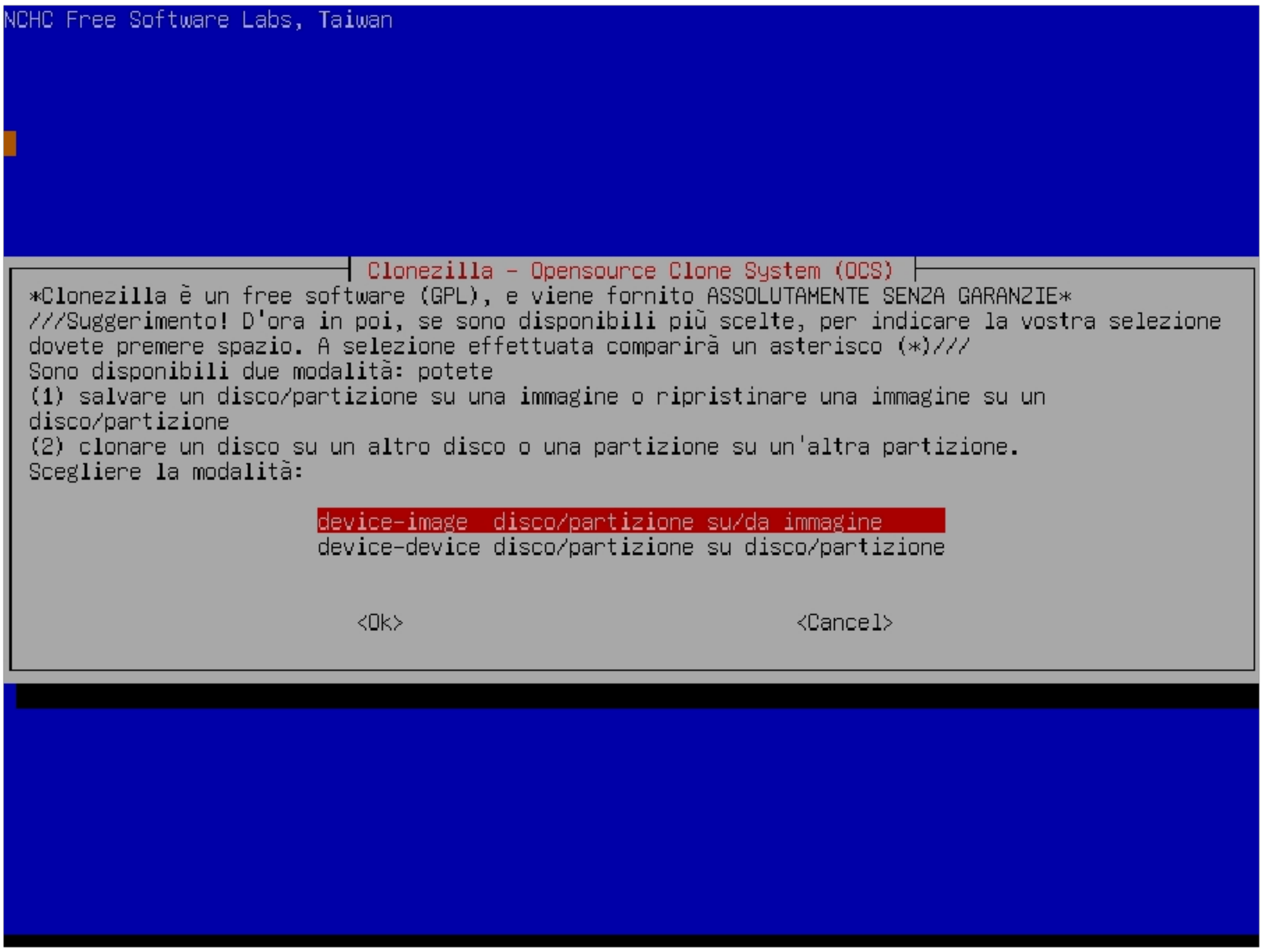
A summary screen will show the available space, press enter to continue:

```
The jobs in /etc/ocs/ocs-live.d/ are finished. Start "ocs-live-general" now.
Preparing the mount point /home/partimag...
Mounting SSH server by:
LC_ALL=C sshfs "clonezilla"@192.168.6.1:"/var/clonezilla/" /home/partimag -p 22
-o nonempty,noatime
The authenticity of host '192.168.6.1 (192.168.6.1)' can't be established.
ECDSA key fingerprint is SHA256:pYBIY9xU/5uwoVVqGG29JhAb6sCxkdOjx798VUD2tiw.
Are you sure you want to continue connecting (yes/no)? yes
clonezilla@192.168.6.1's password:
Utilizzo dello spazio su disco del file system:
**********************************************************************.
SOURCE                                    FSTYPE      SIZE  USED AVAIL USE% TARGET
clonezilla@192.168.6.1:/var/clonezilla/ fuse.sshfs  7,4G  2,4G  4,6G  32% /home/
partimag
**********************************************************************.
Premete "Invio" per continuare ......_
```

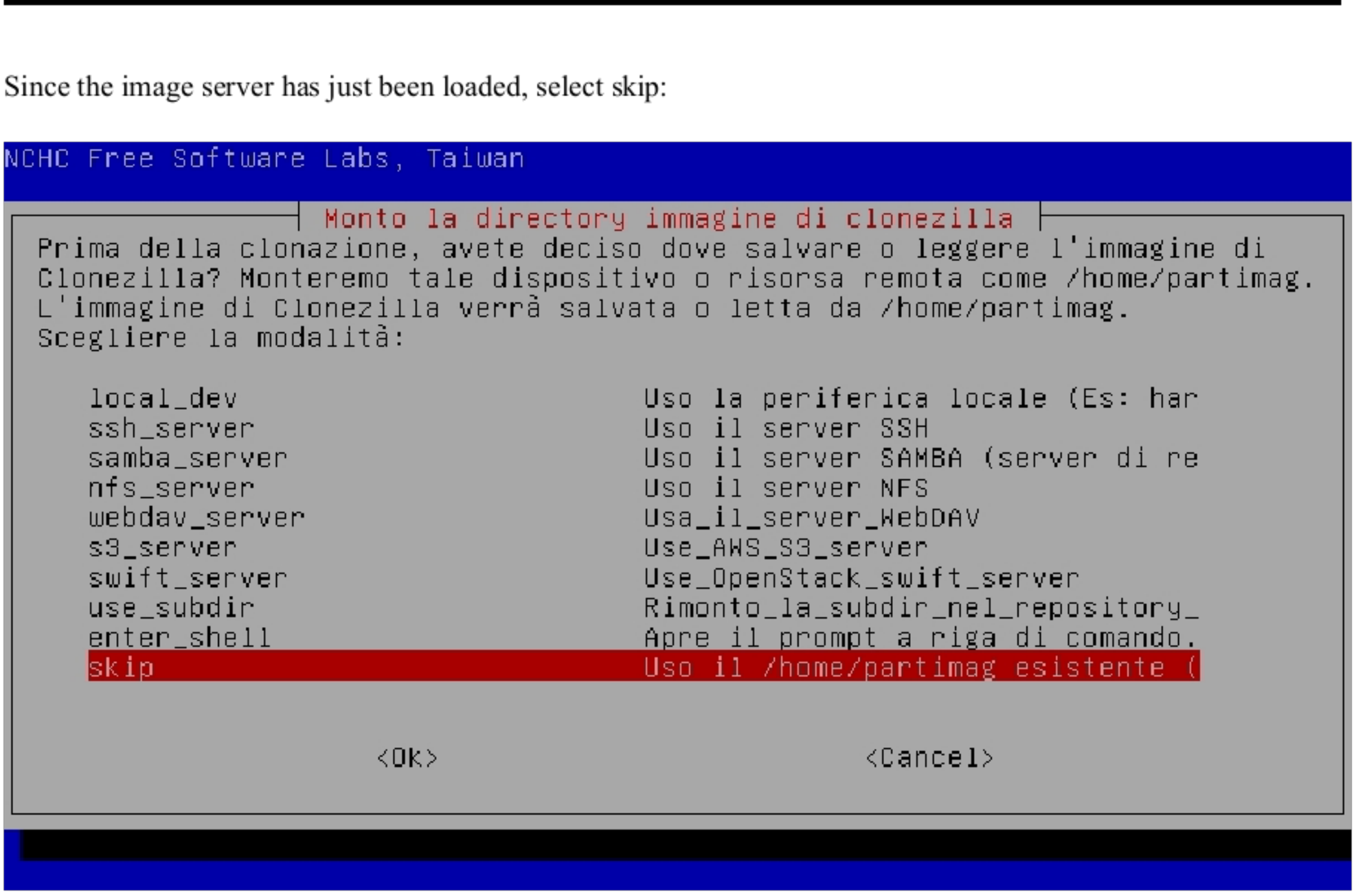
You can then start Clonezilla:



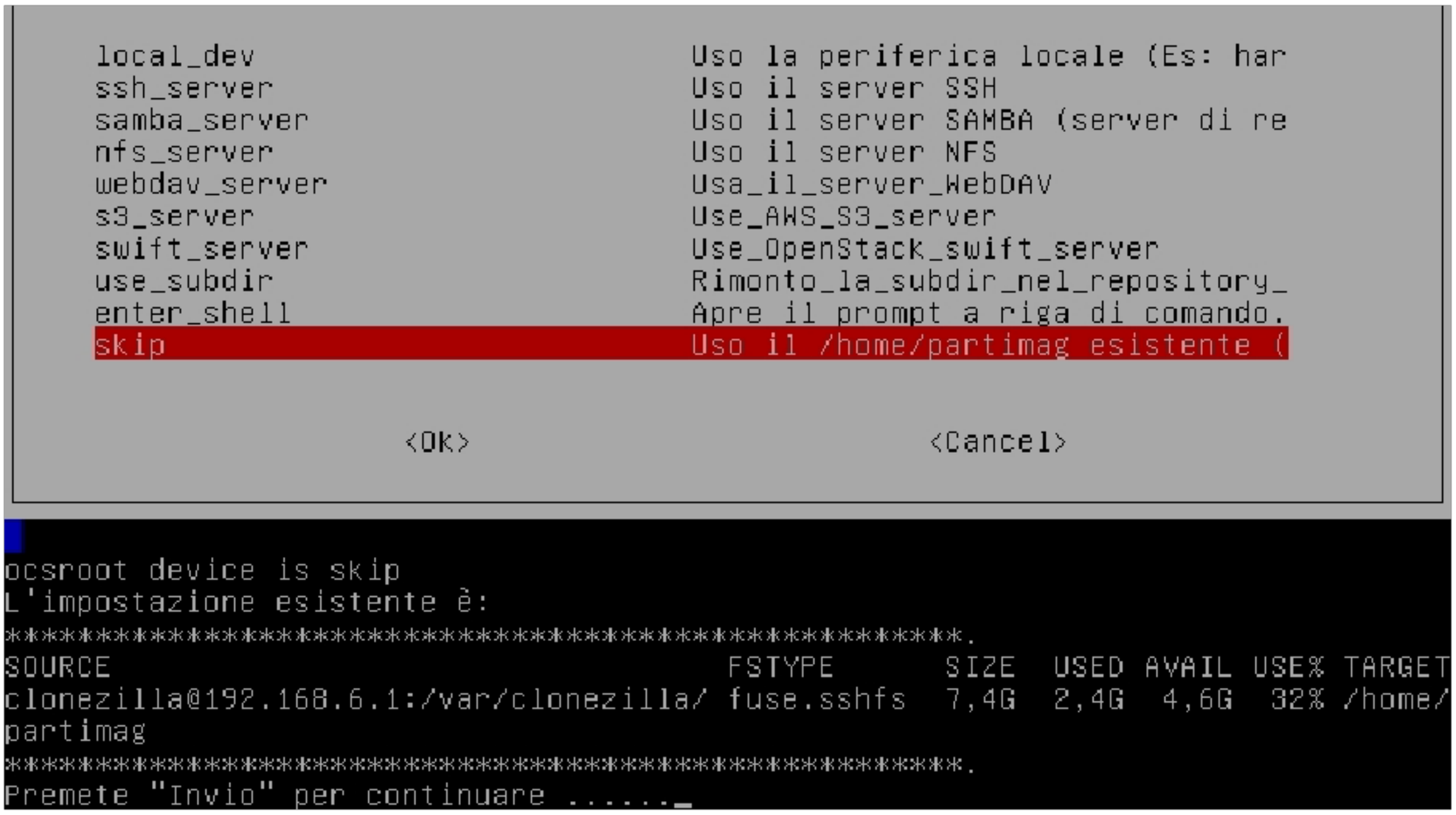
Choose create/restore mode from image (instead of direct copy between computers):



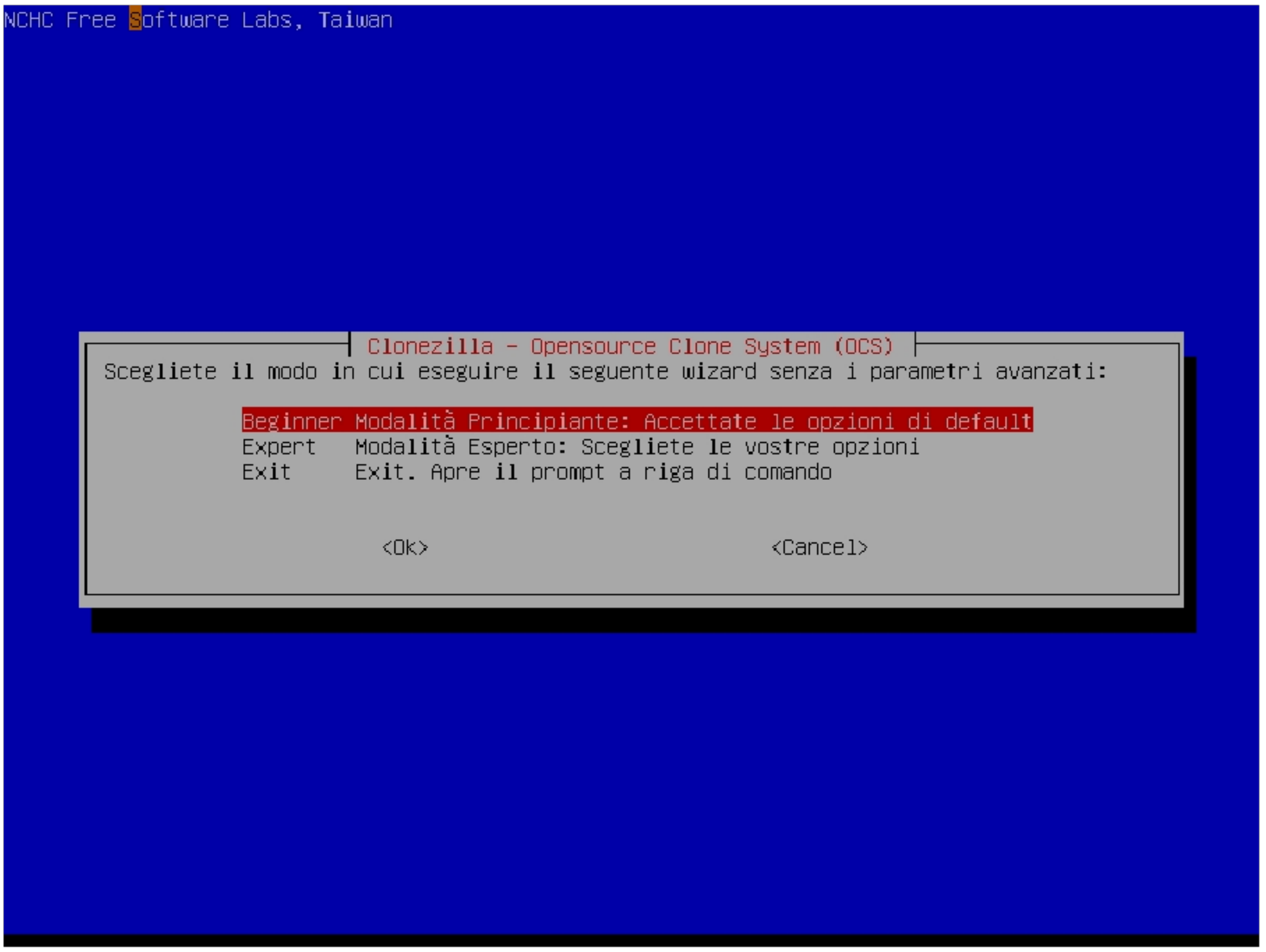
Since the image server has just been loaded, select skip:



And you will be asked for further confirmation, press enter again to continue:

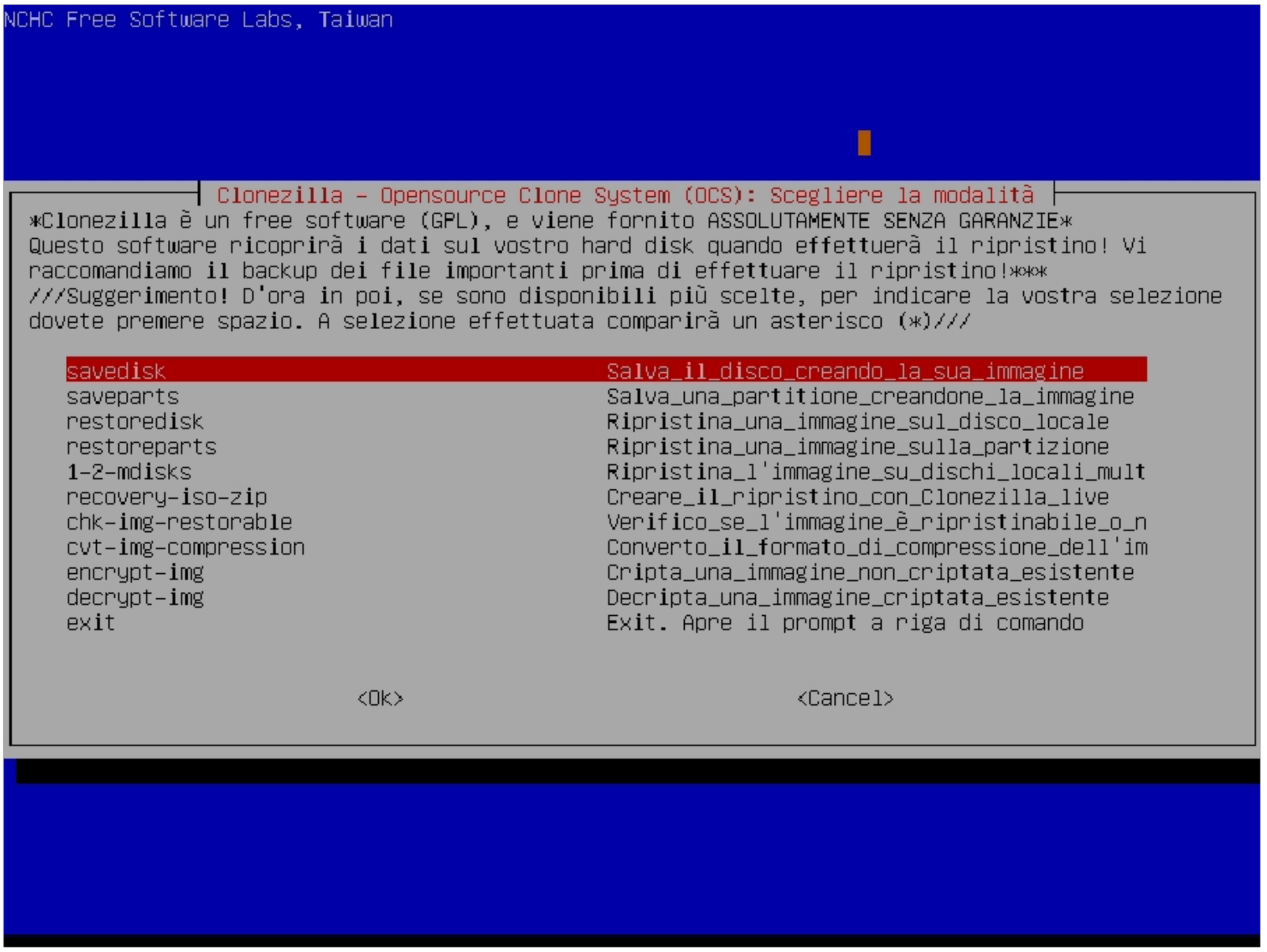


Finally, select beginner mode so that you do not have to provide too many details:

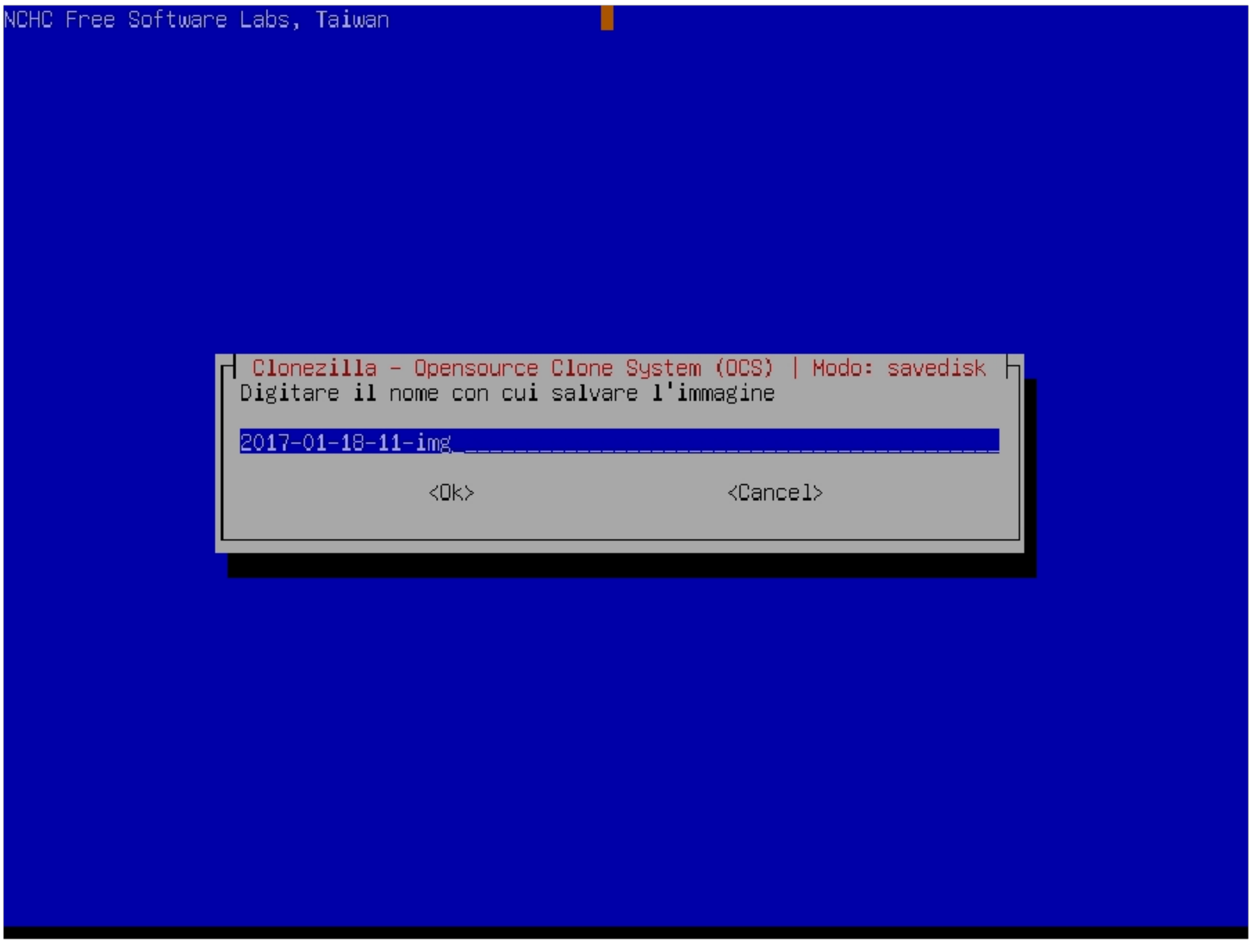


8.5.3 Clone of a machine

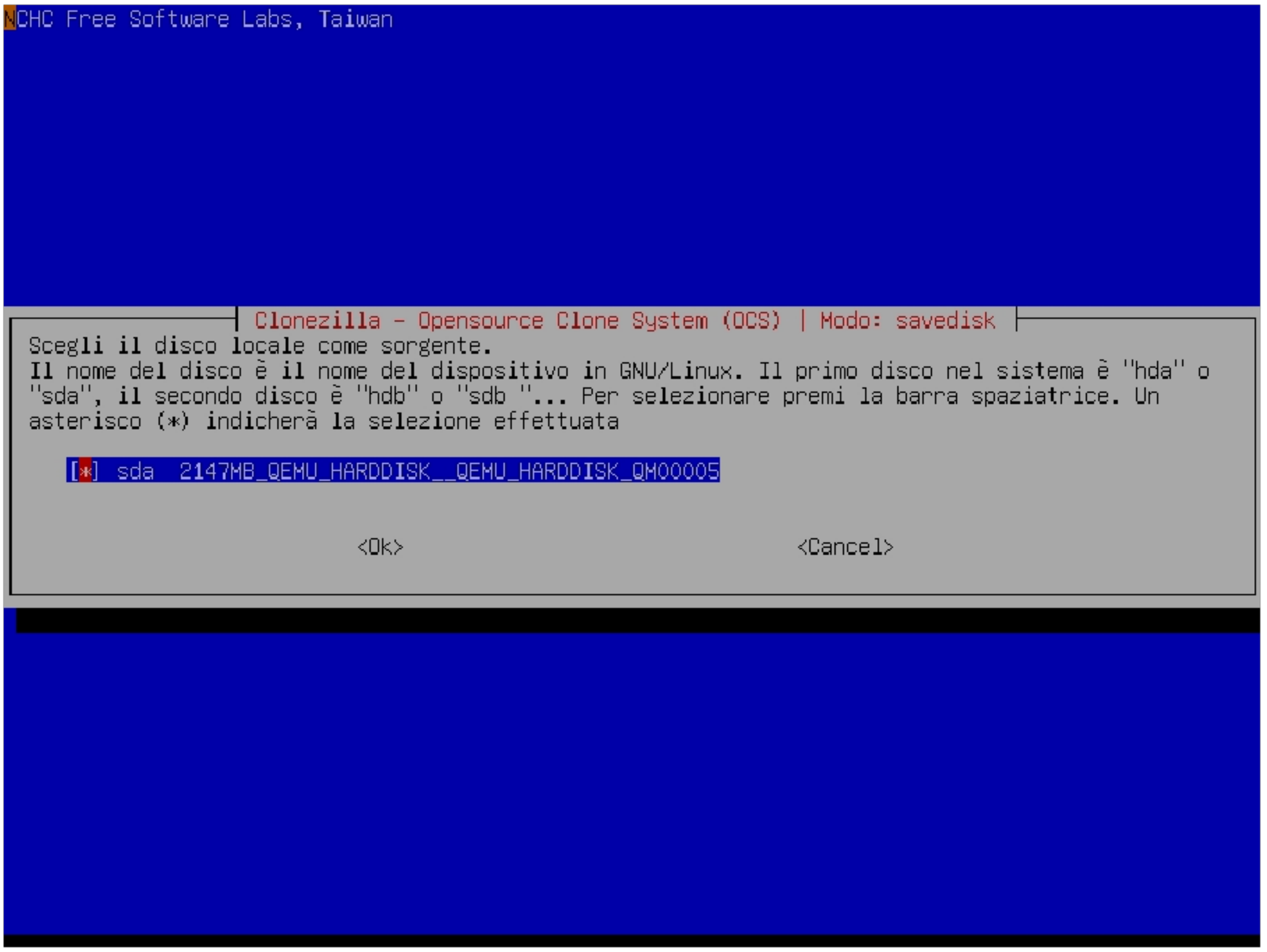
Select the option to create a disk image (note that if this is your first time using clonezilla only the first two choices, "savedisk" and "saveparts" will be presented: all other menu items are enabled when saved images are already present):



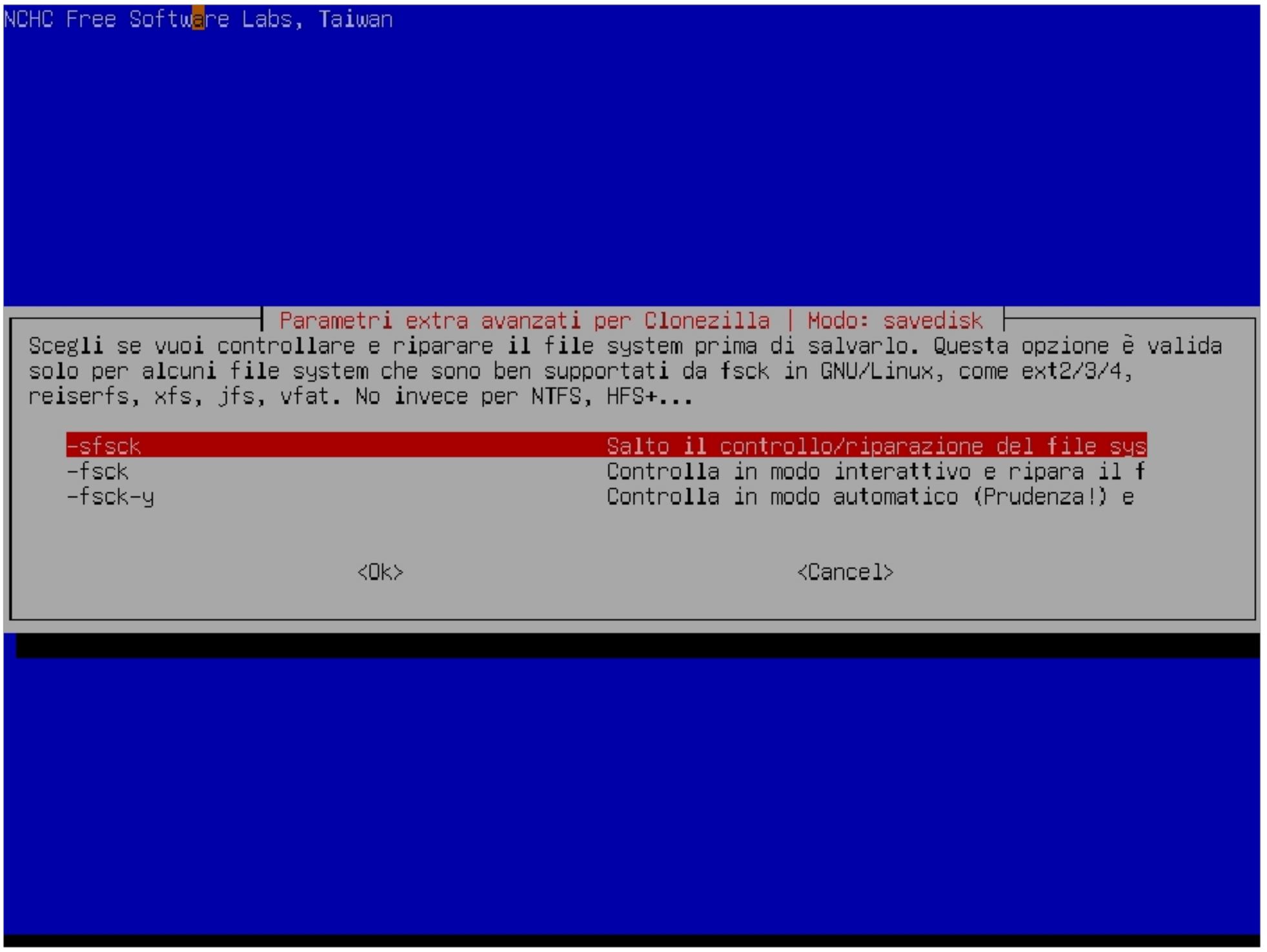
Choose the name to give the image (the default, or something convenient to remember)



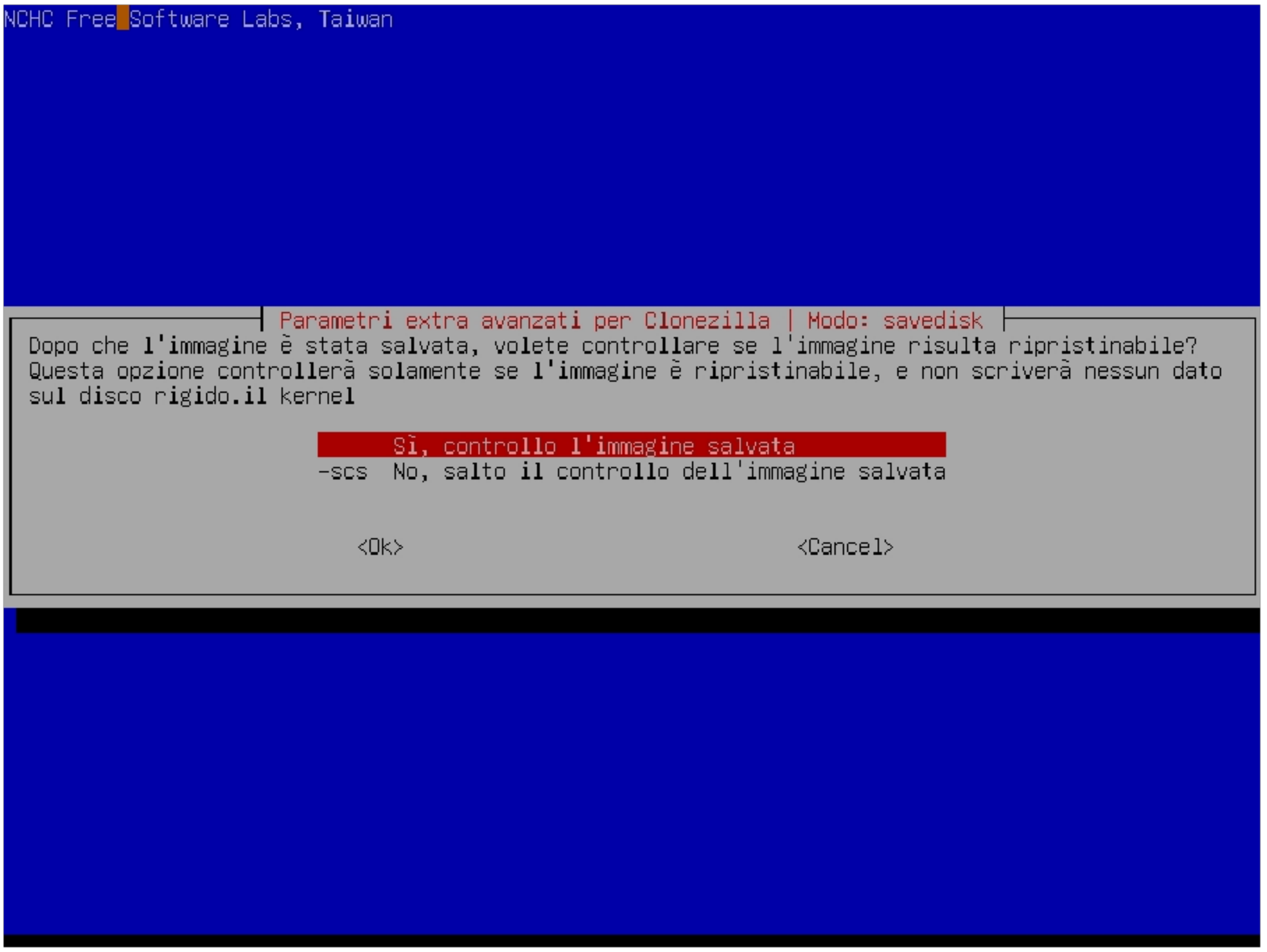
Choose the disk to clone; usually the only one present:



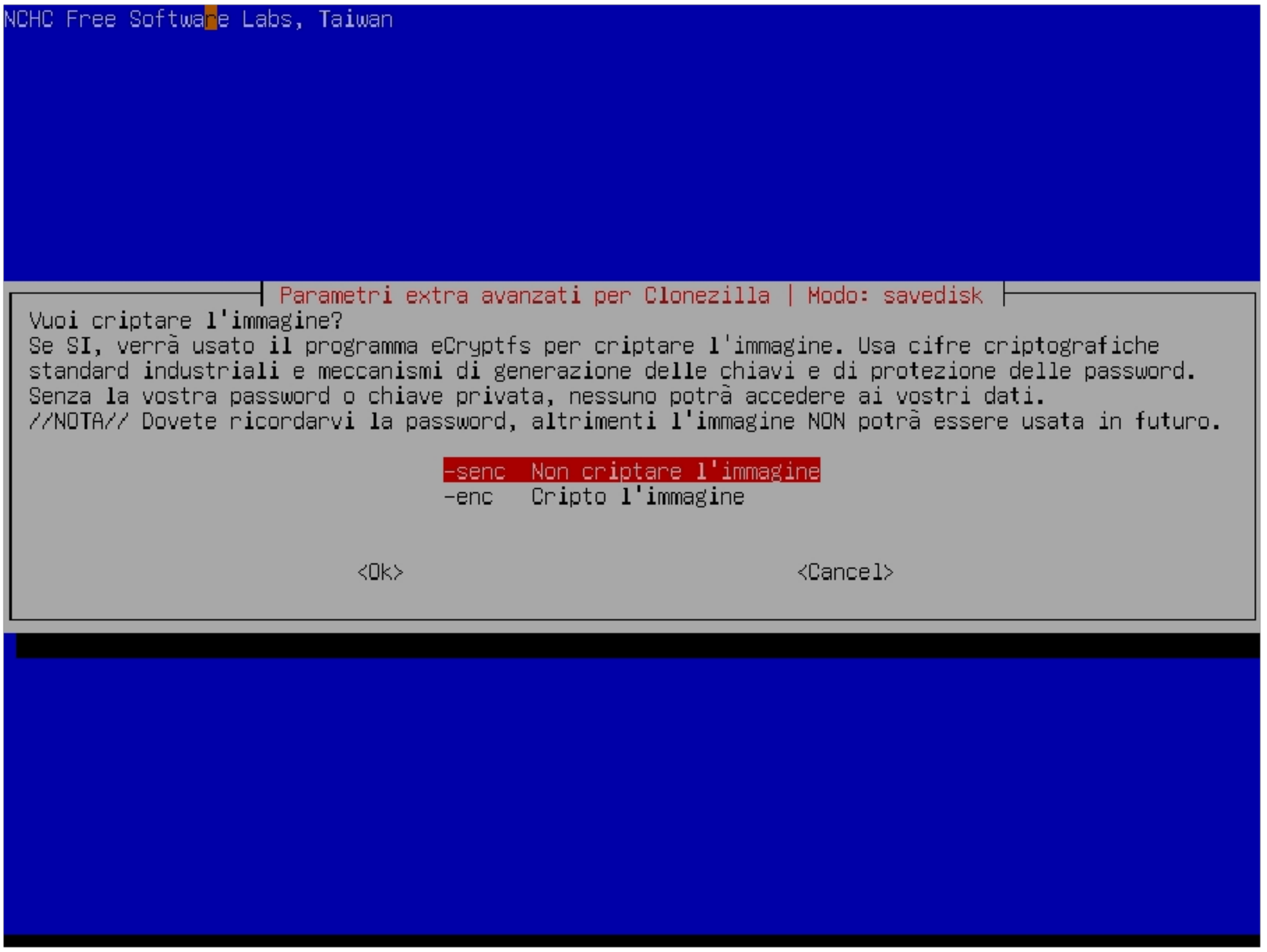
If the machine has been properly shut down, and if it contains windows partitions, choose not to do a filesystem check; it may be useful to do such a check instead if the machine contains only linux partitions and a previous clone attempt has failed:



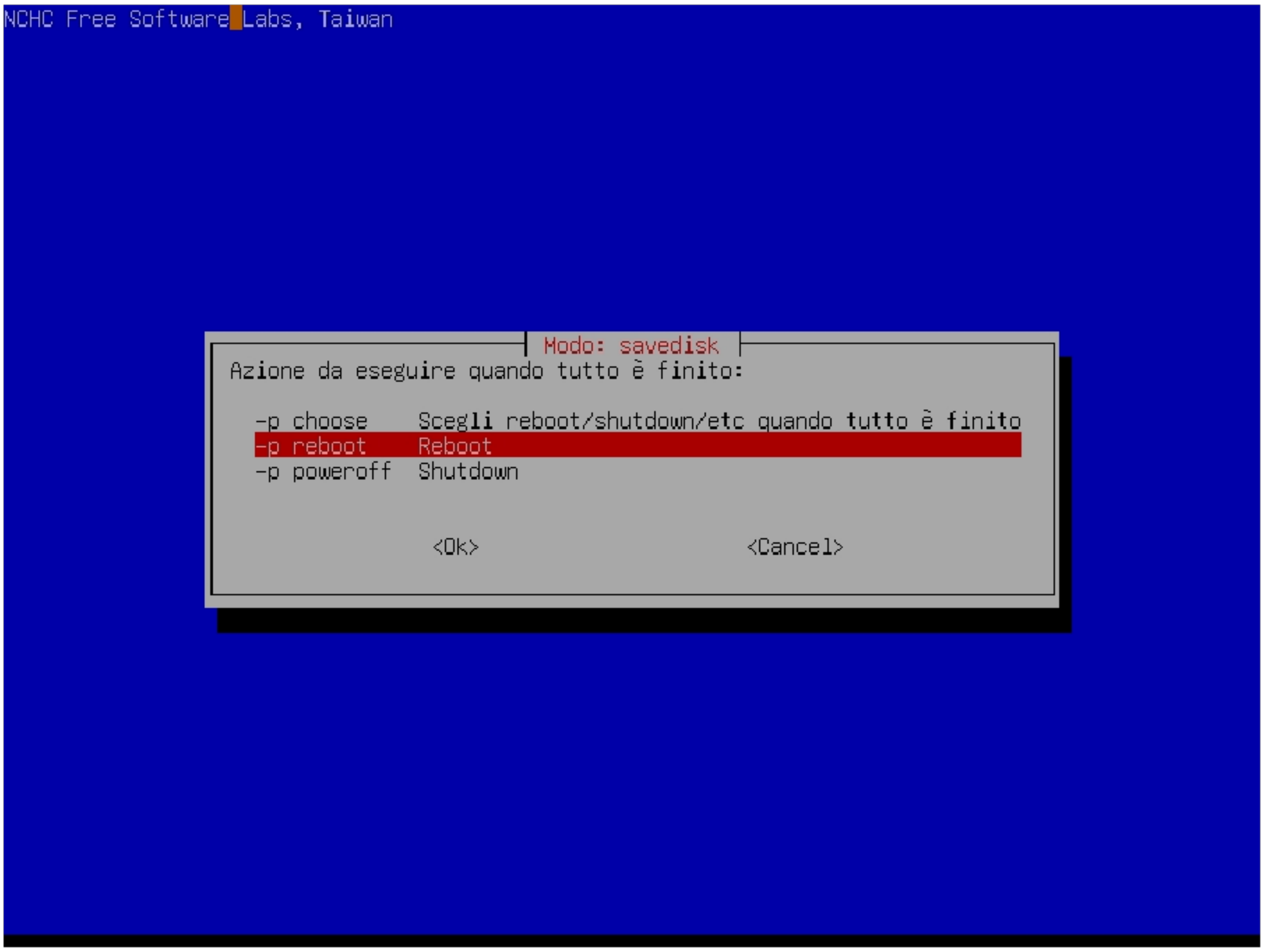
Select to check that the saved image is restorable (default):



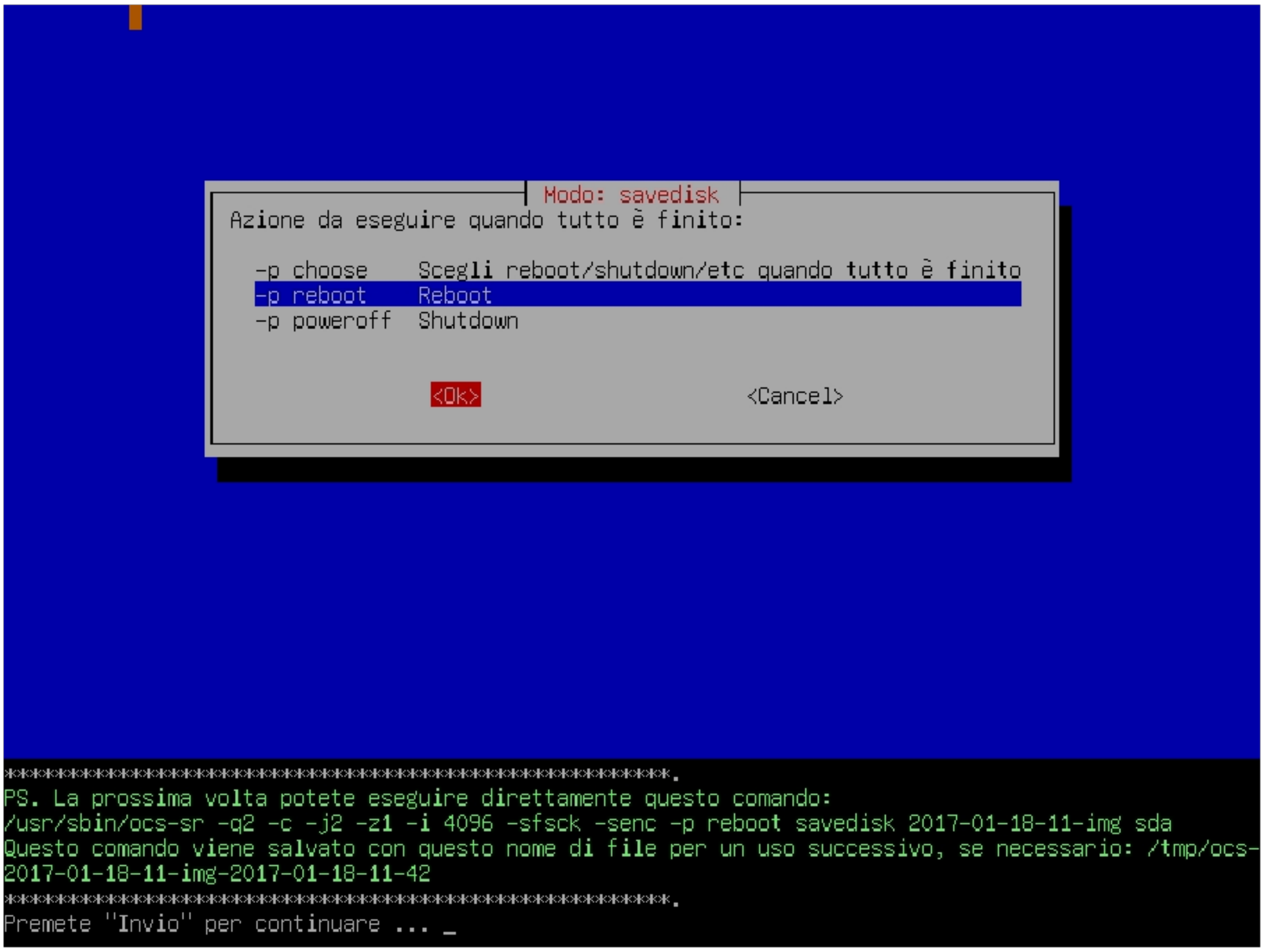
Select not to encrypt the image; not necessary since it is saved on the fuss-server:



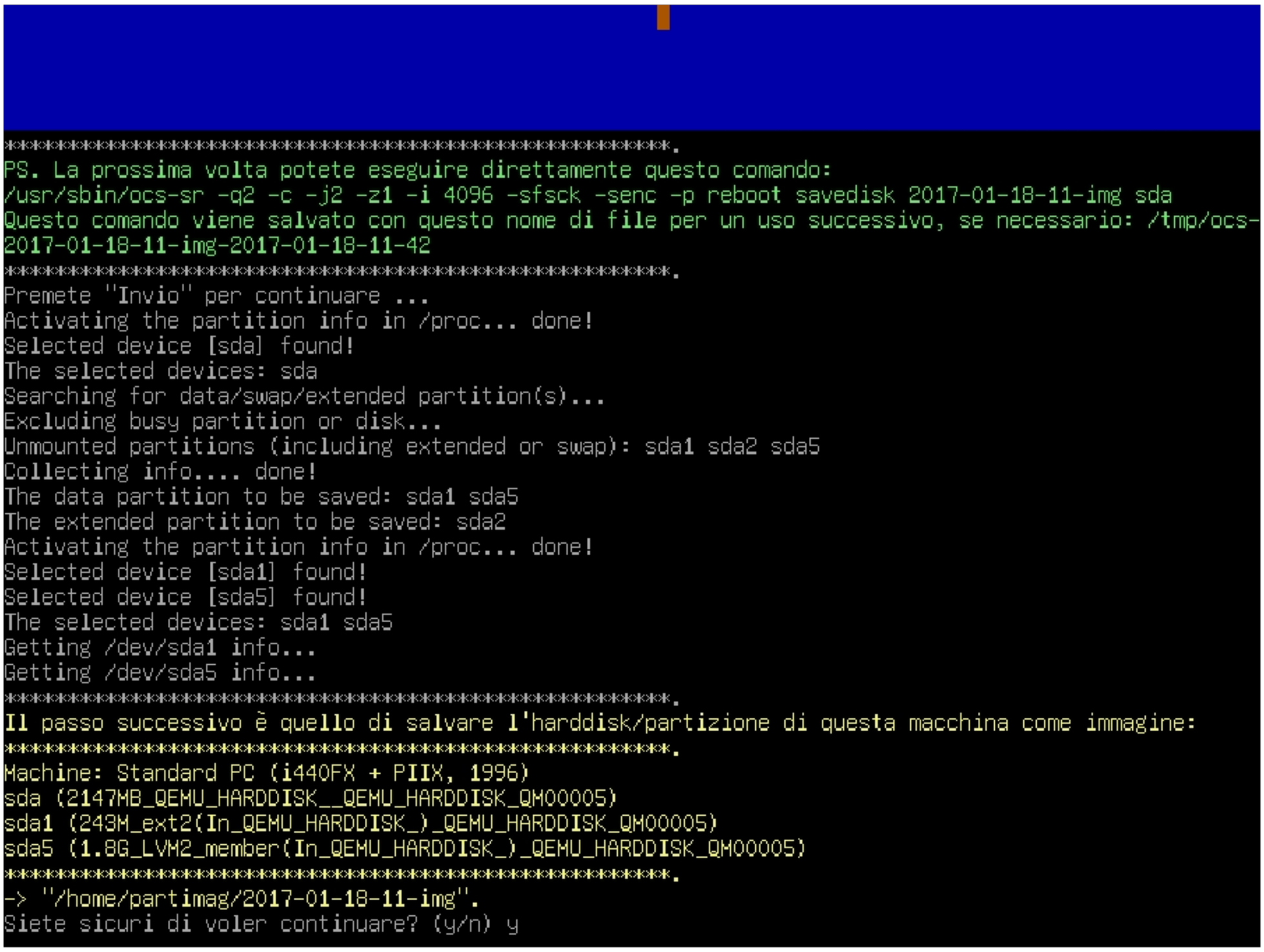
Select to restart the computer at the end of copying:



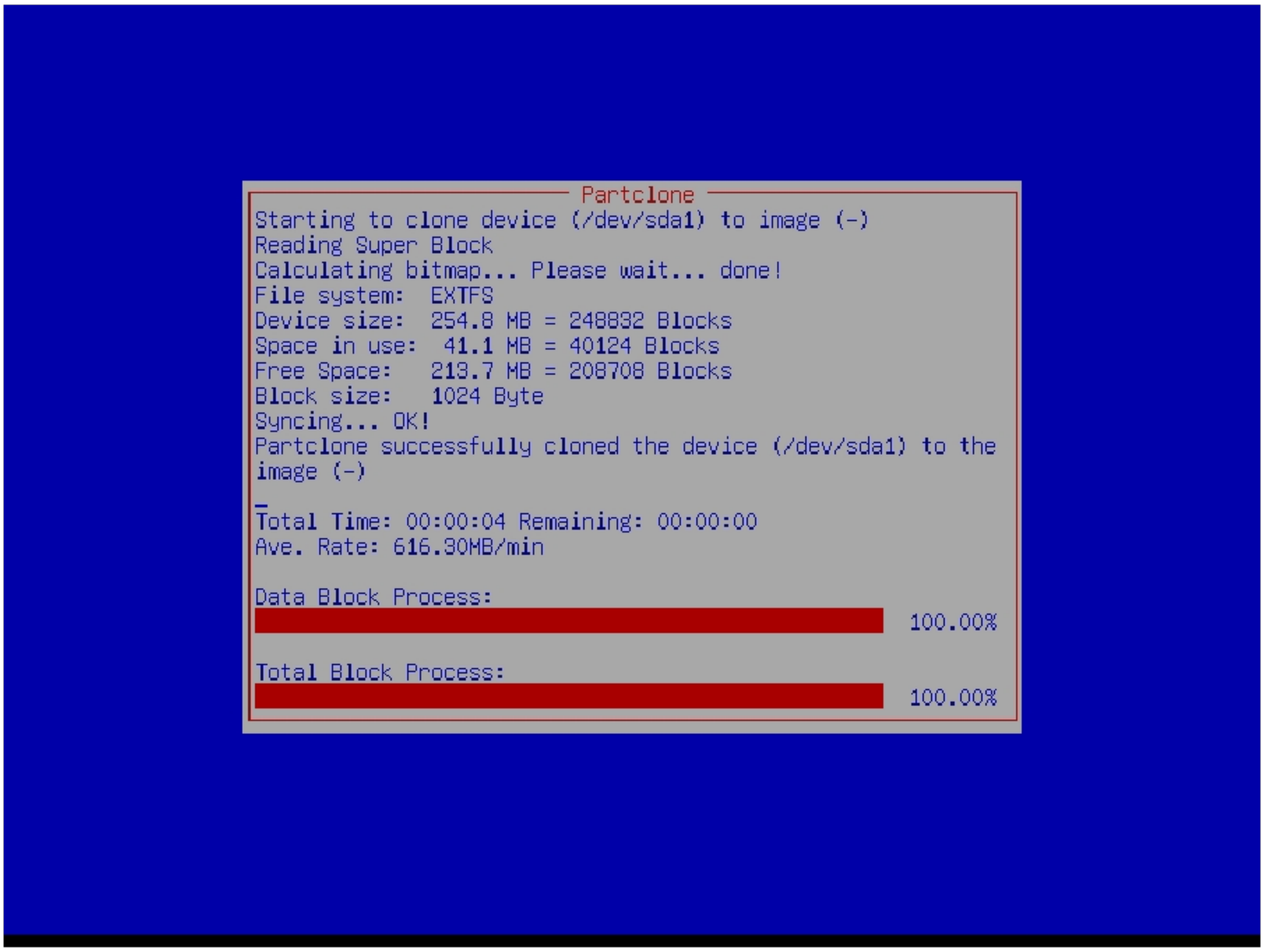
Clonezilla will now show the complete command line that will be executed; press enter to continue:



You are asked to confirm to proceed, type `y` to continue:



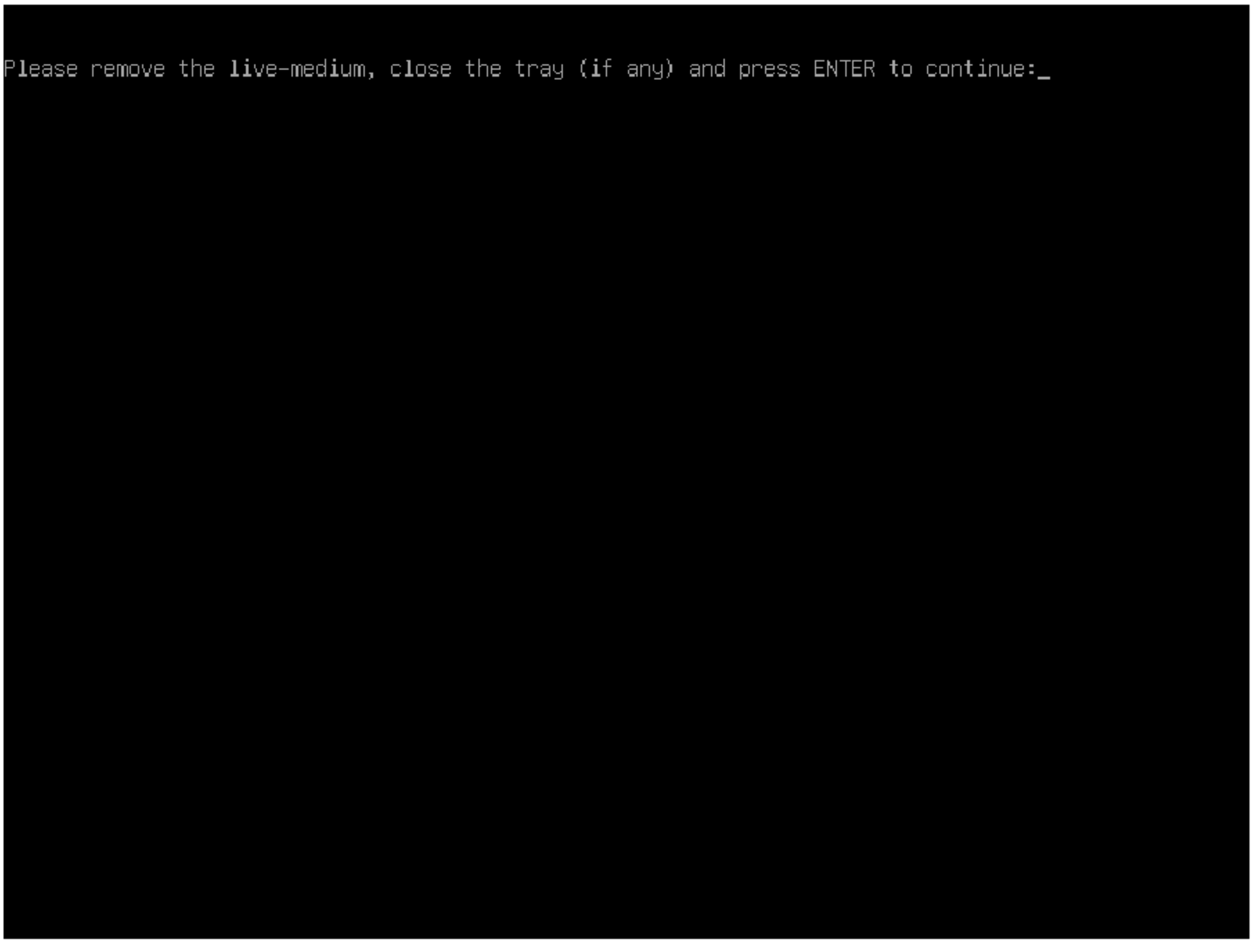
Clonezilla will proceed to create an image and save it



To the point of announcing that it is ready for a reboot:

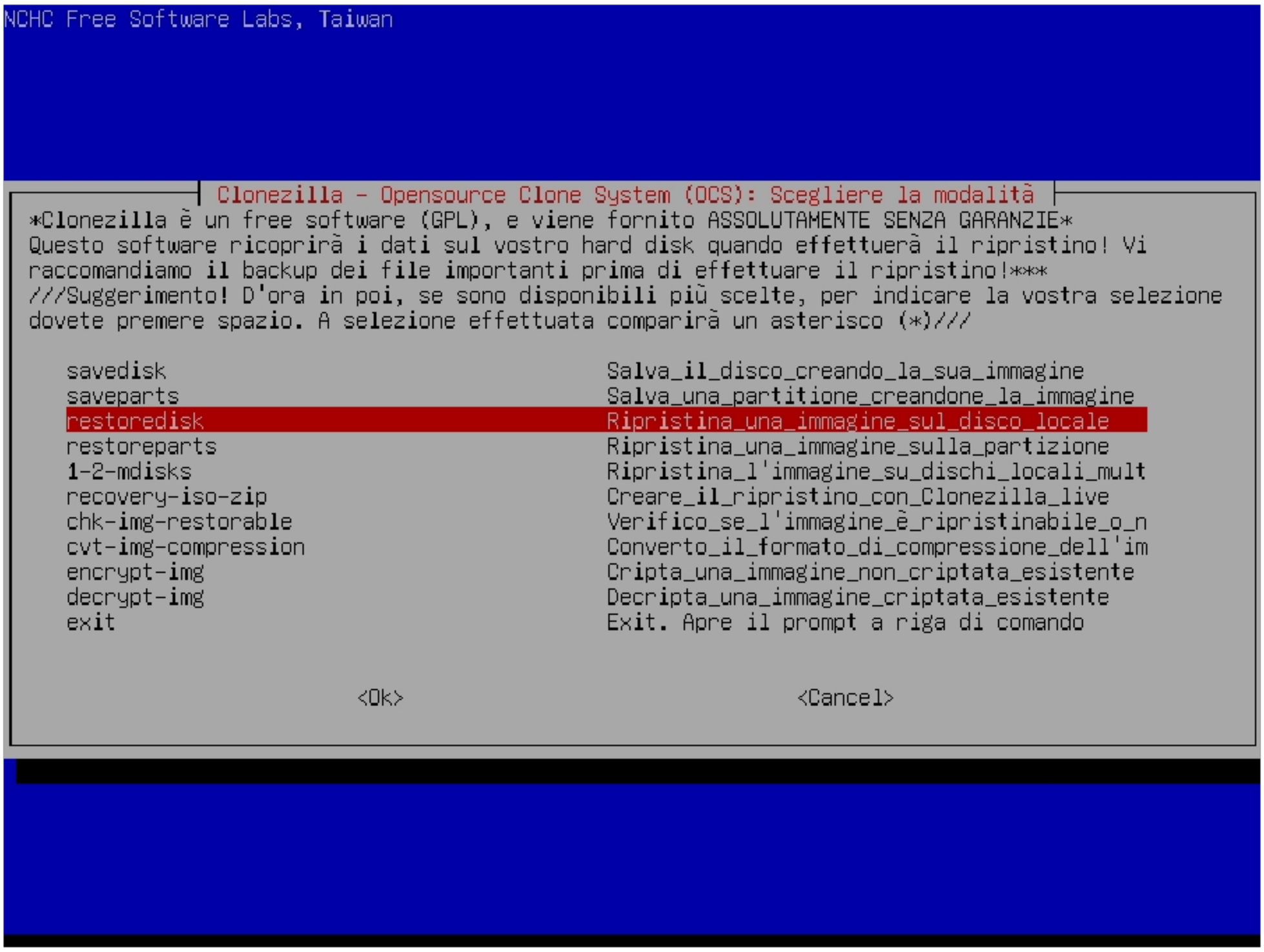
```
Checked successfully.
L'immagine di questa partizione è ripristinabile: debian-vg-root
*************************************************.
*************************************************.
Found the swap partition /dev/debian-vg/swap_1 info:
UUID="9931857e-2704-4e35-8a96-6c8a1ac4b2ba"
LABEL=""
Swap partition info file found!
*************************************************.
*************************************************.
Tutte le immagini di partizione o dispositivi LV in questa immagine sono stati controllati e risulta
no ripristinabili: 2017-01-18-11-img
Summary of image checking:
==========================
Partition table file for disk was found: sda
MBR file for this disk was found: sda
L'immagine di questa partizione è ripristinabile: sda1
L'immagine di questa partizione è ripristinabile: debian-vg-root
Tutte le immagini di partizione o dispositivi LV in questa immagine sono stati controllati e risulta
no ripristinabili: 2017-01-18-11-img
==========================
*************************************************
*************************************************
Checking if udevd rules have to be restored...
This program is not started by Clonezilla server, so skip notifying it the job is done.
Finished!
Now syncing - flush filesystem buffers...
Ending /usr/sbin/ocs-sr at 2017-01-18 11:48:34 UTC...
"ocs-live-general" finished.
Check /var/log/clonezilla.log for more details.
The next step: reboot
Trying to unmount /home/partimag... done!
Will reboot (Press Ctrl-C to abort)... 7 6 5 4 3 2 _
```

Finally, press enter to allow the reboot (since clonezilla was started over the network, no disk needs to be removed):

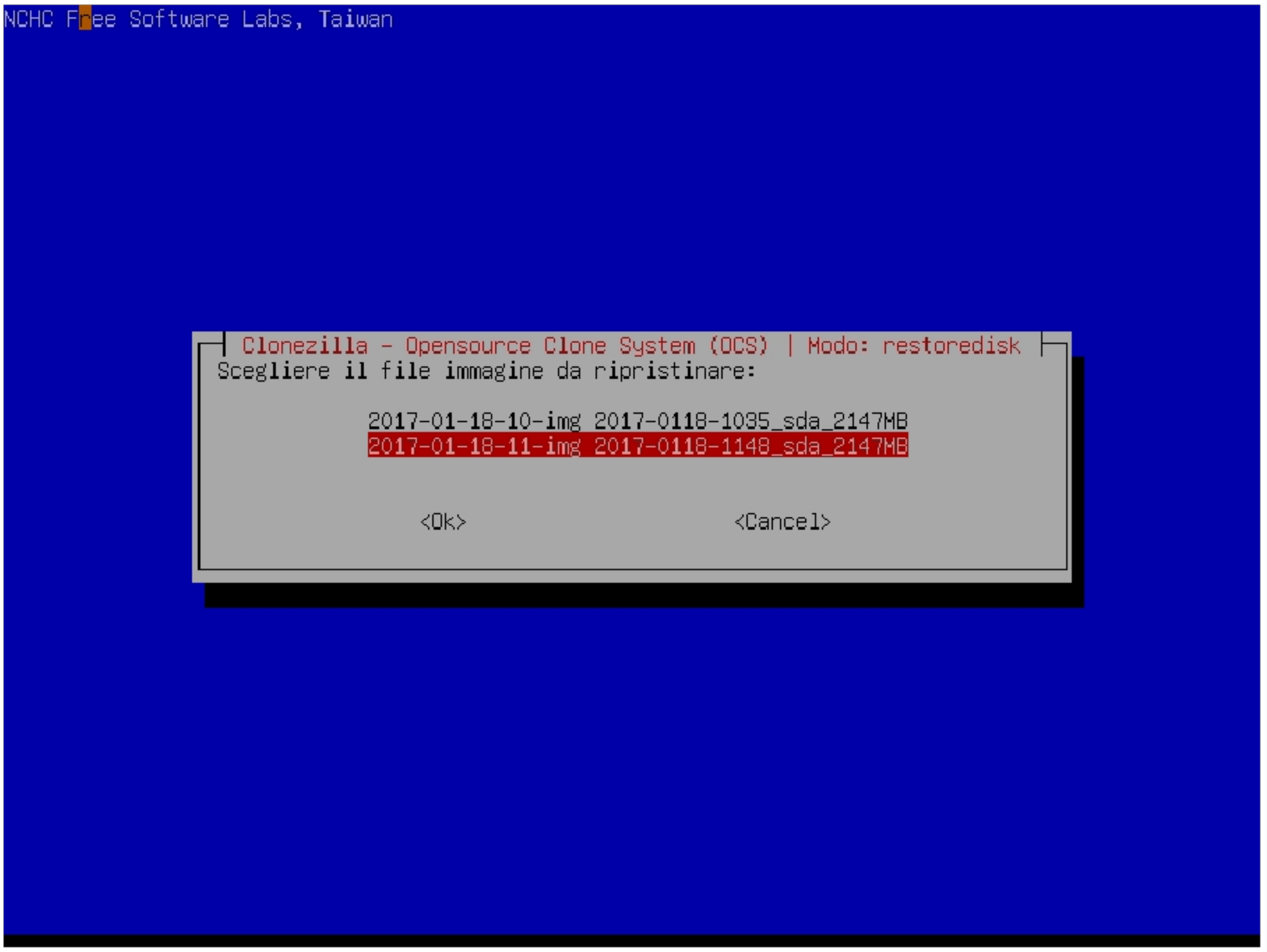


8.5.4 Restoring a machine

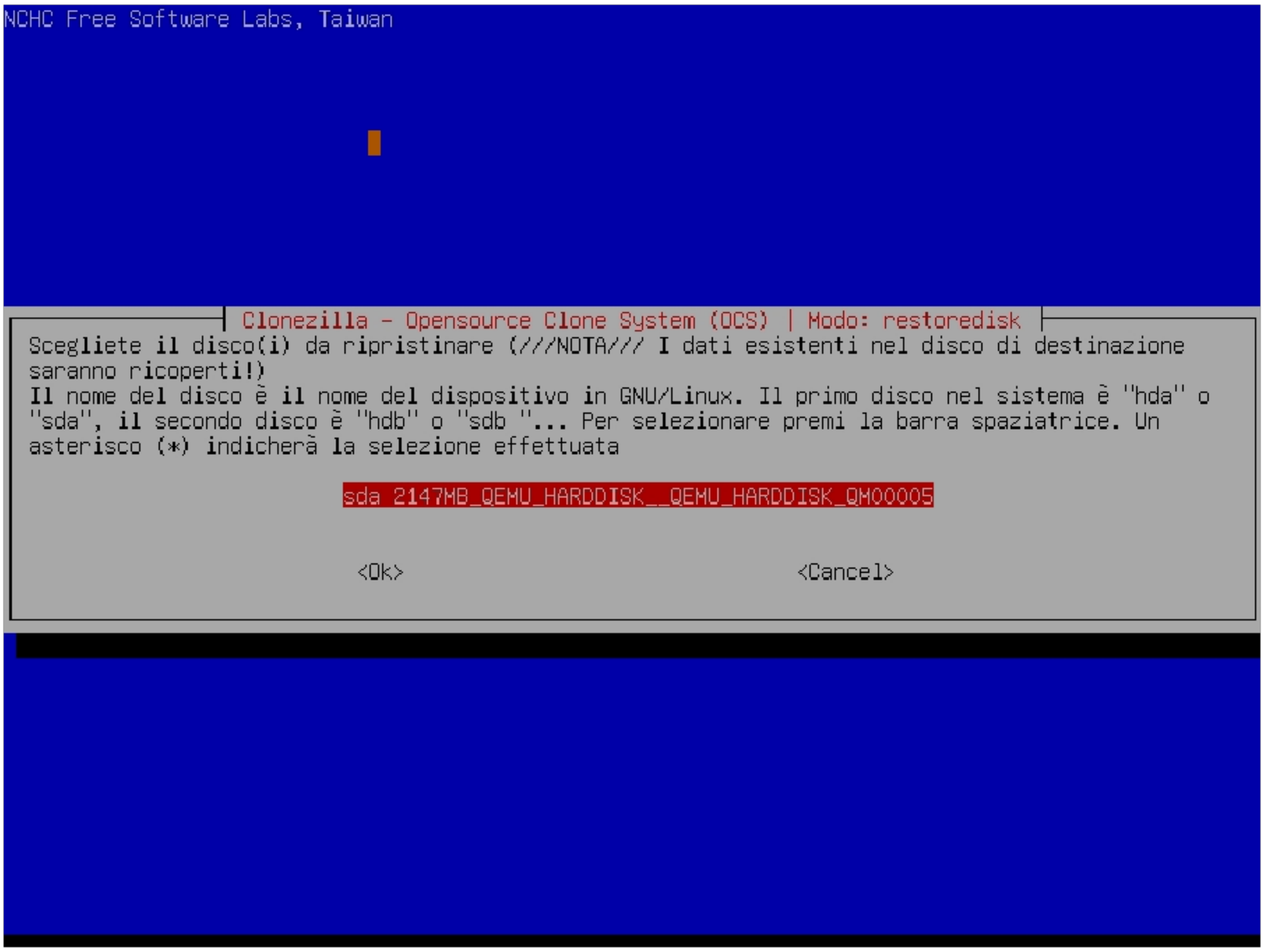
Select the option to restore an image from disk:



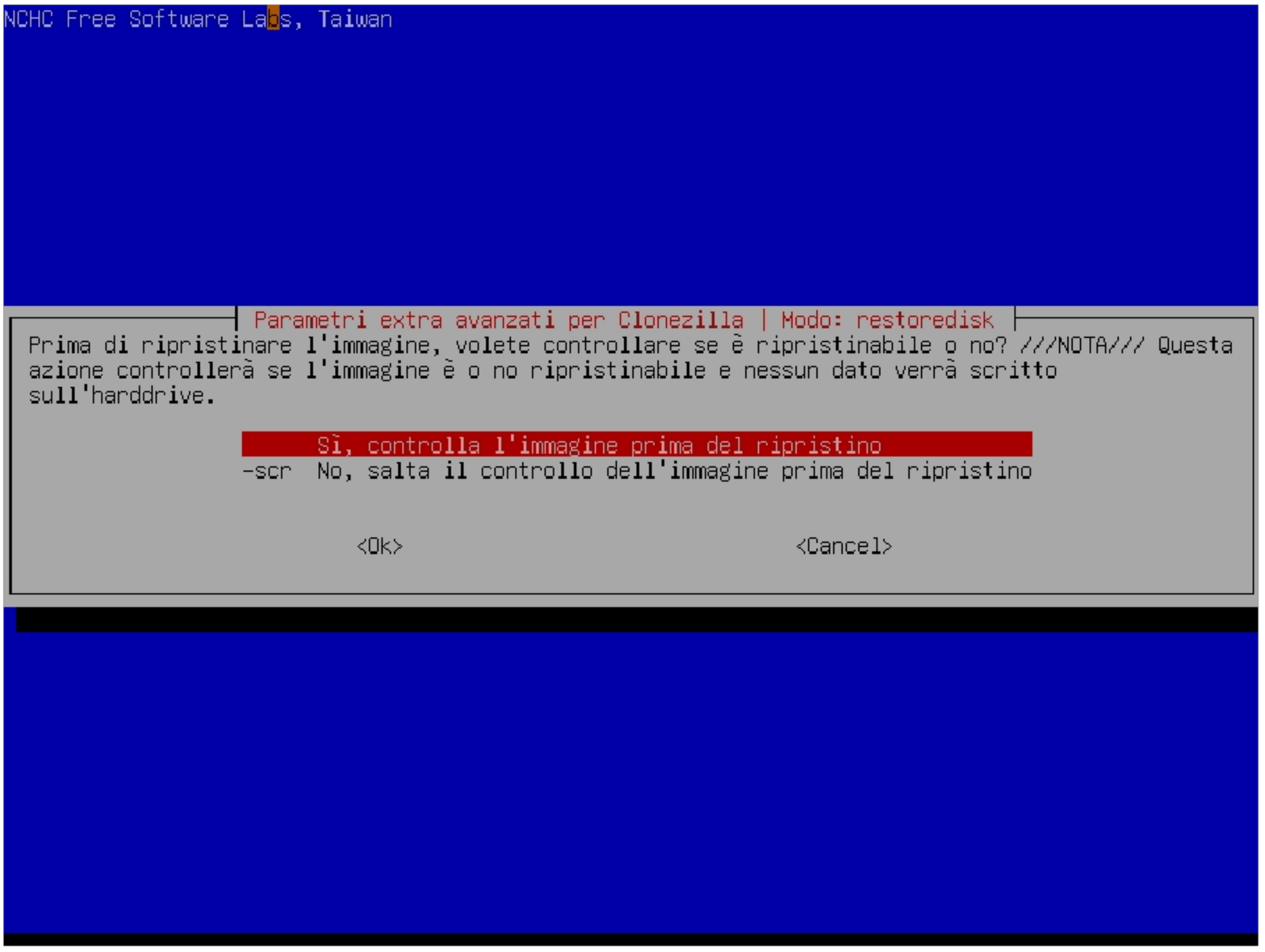
Select the name of the image; if there is more than one, it is necessary to remember the name given during creation:



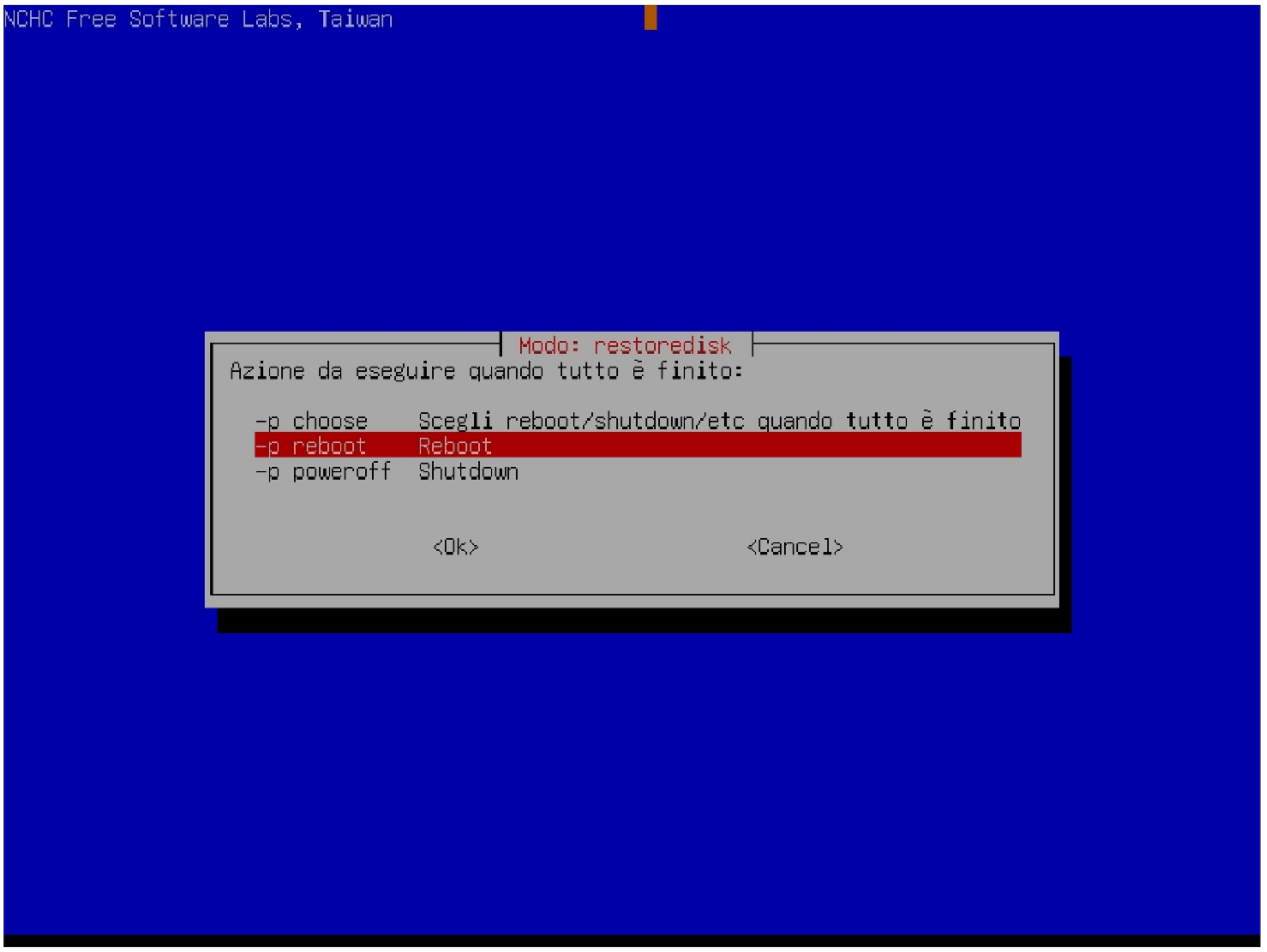
Select the disk to restore the image to; usually the only one present:



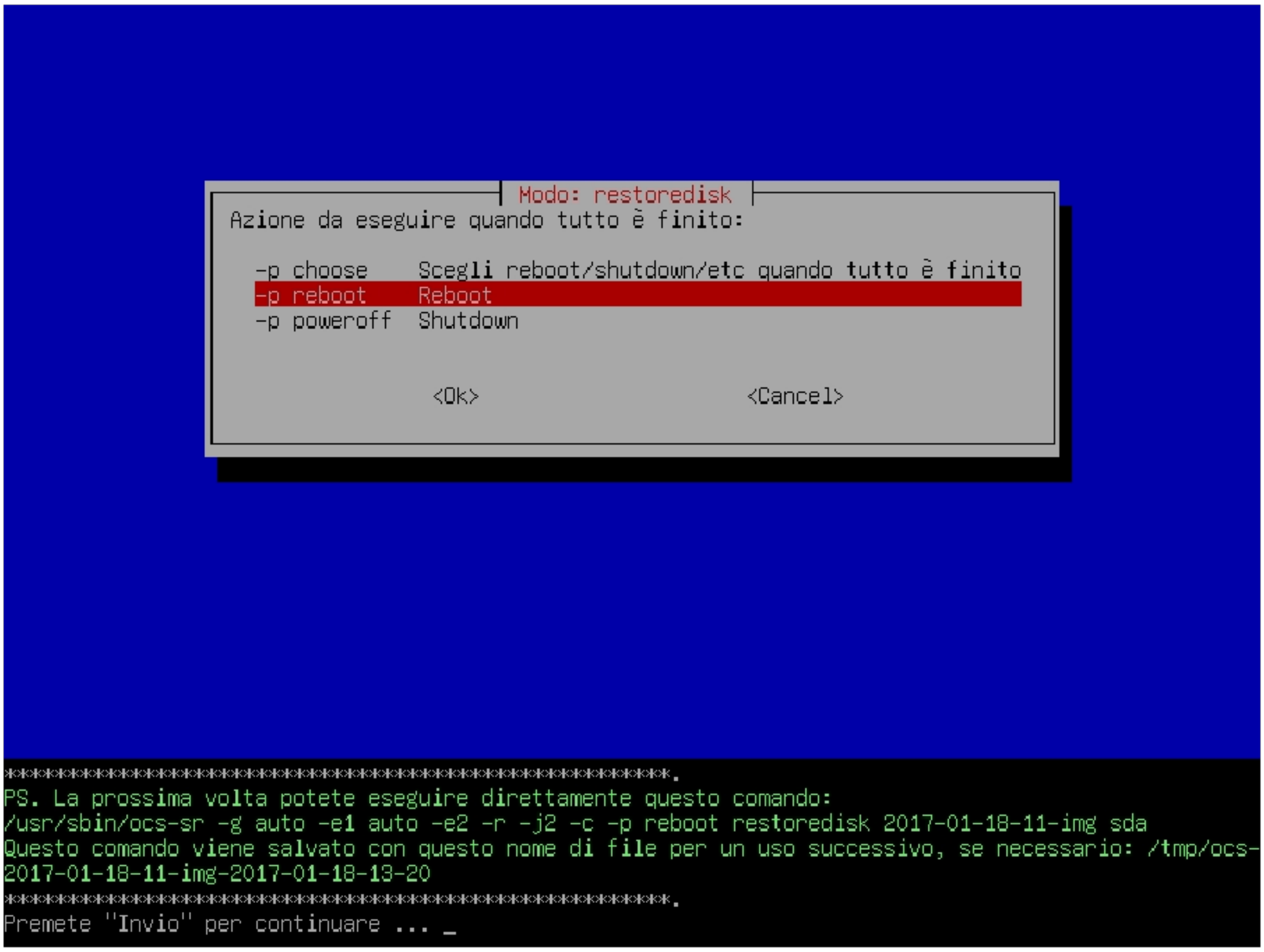
Select to verify the image before restoring:



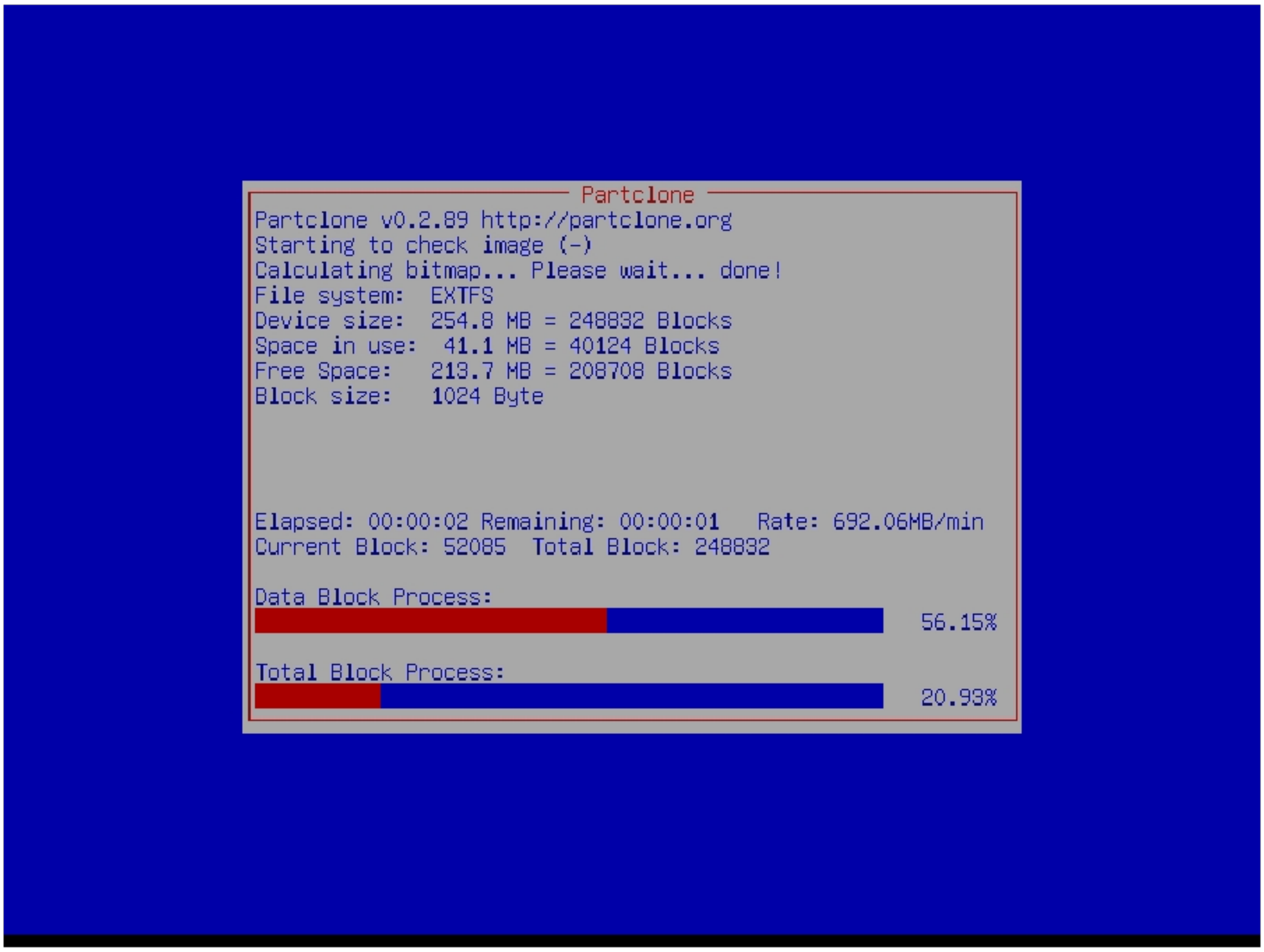
Select to restart the computer at the end of the recovery:



Clonezilla will now show the complete command line that will be executed; press enter to continue:



Clonezilla will begin to verify the selected image:

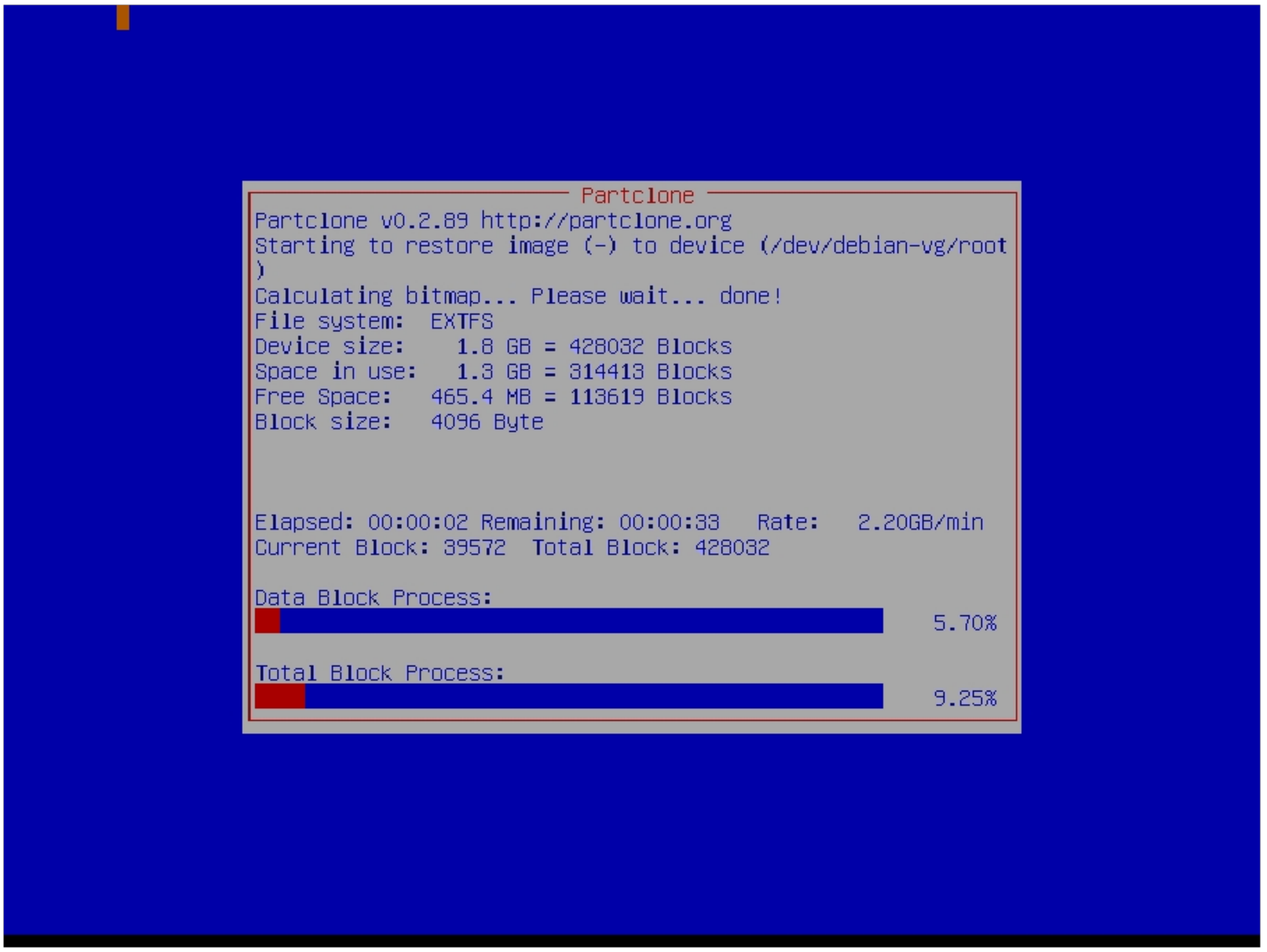


It will then ask twice for confirmation that it wants to continue, deleting anything that may be on the local disk:

```
**************************************************.
**************************************************.
Found the swap partition /dev/debian-vg/swap_1 info:
UUID=''9931857e-2704-4e35-8a96-6c8a1ac4b2ba''
LABEL=''''
Swap partition info file found!
**************************************************.
**************************************************.
Tutte le immagini di partizione o dispositivi LV in questa immagine sono stati controllati e risulta
no ripristinabili: 2017-01-18-11-img
Summary of image checking:
==========================
Partition table file for disk was found: sda
MBR file for this disk was found: sda
L'immagine di questa partizione è ripristinabile: sda1
L'immagine di questa partizione è ripristinabile: debian-vg-root
Tutte le immagini di partizione o dispositivi LV in questa immagine sono stati controllati e risulta
no ripristinabili: 2017-01-18-11-img
==========================
Activating the partition info in /proc... done!
Getting /dev/sda1 info...
Getting /dev/sda2 info...
Getting /dev/sda5 info...
**************************************************.
Il passo successivo è quello di ripristinare l'immagine nell'harddisk/partizione di questa macchina:
 ''/home/partimag/2017-01-18-11-img'' -> ''sda sda1 sda5''
L'immagine è stata creata a: 2017-0118-1148
ATTENZIONE!!! ATTENZIONE!!! ATTENZIONE!!!
ATTENZIONE. I DATI ESISTENTI IN QUESTO HARDDISK/PARTIZIONE(I), VERRANNO RICOPERTI! TUTTI I DATI ESIS
TENTI ANDRANNO PERSI:
**************************************************.
Machine: Standard PC (i440FX + PIIX, 1996)
sda (2147MB_QEMU_HARDDISK__QEMU_HARDDISK_QM00005)
sda1 (243M_ext2(In_QEMU_HARDDISK_)_QEMU_HARDDISK_QM00005)
sda5 (1.8G_LVM2_member(In_QEMU_HARDDISK_)_QEMU_HARDDISK_QM00005)
**************************************************.
Siete sicuri di voler continuare? (y/n) y_
```

```
no ripristinabili: 2017-01-18-11-img
==========================
Activating the partition info in /proc... done!
Getting /dev/sda1 info...
Getting /dev/sda2 info...
Getting /dev/sda5 info...
**************************************************.
Il passo successivo è quello di ripristinare l'immagine nell'harddisk/partizione di questa macchina:
 ''/home/partimag/2017-01-18-11-img'' -> ''sda sda1 sda5''
L'immagine è stata creata a: 2017-0118-1148
ATTENZIONE!!! ATTENZIONE!!! ATTENZIONE!!!
ATTENZIONE. I DATI ESISTENTI IN QUESTO HARDDISK/PARTIZIONE(I), VERRANNO RICOPERTI! TUTTI I DATI ESIS
TENTI ANDRANNO PERSI:
**************************************************.
Machine: Standard PC (i440FX + PIIX, 1996)
sda (2147MB_QEMU_HARDDISK__QEMU_HARDDISK_QM00005)
sda1 (243M_ext2(In_QEMU_HARDDISK_)_QEMU_HARDDISK_QM00005)
sda5 (1.8G_LVM2_member(In_QEMU_HARDDISK_)_QEMU_HARDDISK_QM00005)
**************************************************.
Siete sicuri di voler continuare? (y/n) y
OK, è partito!!
This program is not started by clonezilla server.
**************************************************.
Permettetemi di chiedervi ancora una volta.
Il passo successivo è quello di ripristinare l'immagine nell'harddisk/partizione di questa macchina:
 ''/home/partimag/2017-01-18-11-img'' -> ''sda sda1 sda5''
L'immagine è stata creata a: 2017-0118-1148
ATTENZIONE!!! ATTENZIONE!!! ATTENZIONE!!!
ATTENZIONE. I DATI ESISTENTI IN QUESTO HARDDISK/PARTIZIONE(I), VERRANNO RICOPERTI! TUTTI I DATI ESIS
TENTI ANDRANNO PERSI:
**************************************************.
Machine: Standard PC (i440FX + PIIX, 1996)
sda (2147MB_QEMU_HARDDISK__QEMU_HARDDISK_QM00005)
sda1 (243M_ext2(In_QEMU_HARDDISK_)_QEMU_HARDDISK_QM00005)
sda5 (1.8G_LVM2_member(In_QEMU_HARDDISK_)_QEMU_HARDDISK_QM00005)
**************************************************.
Siete sicuri di voler continuare? (y/n) y
```

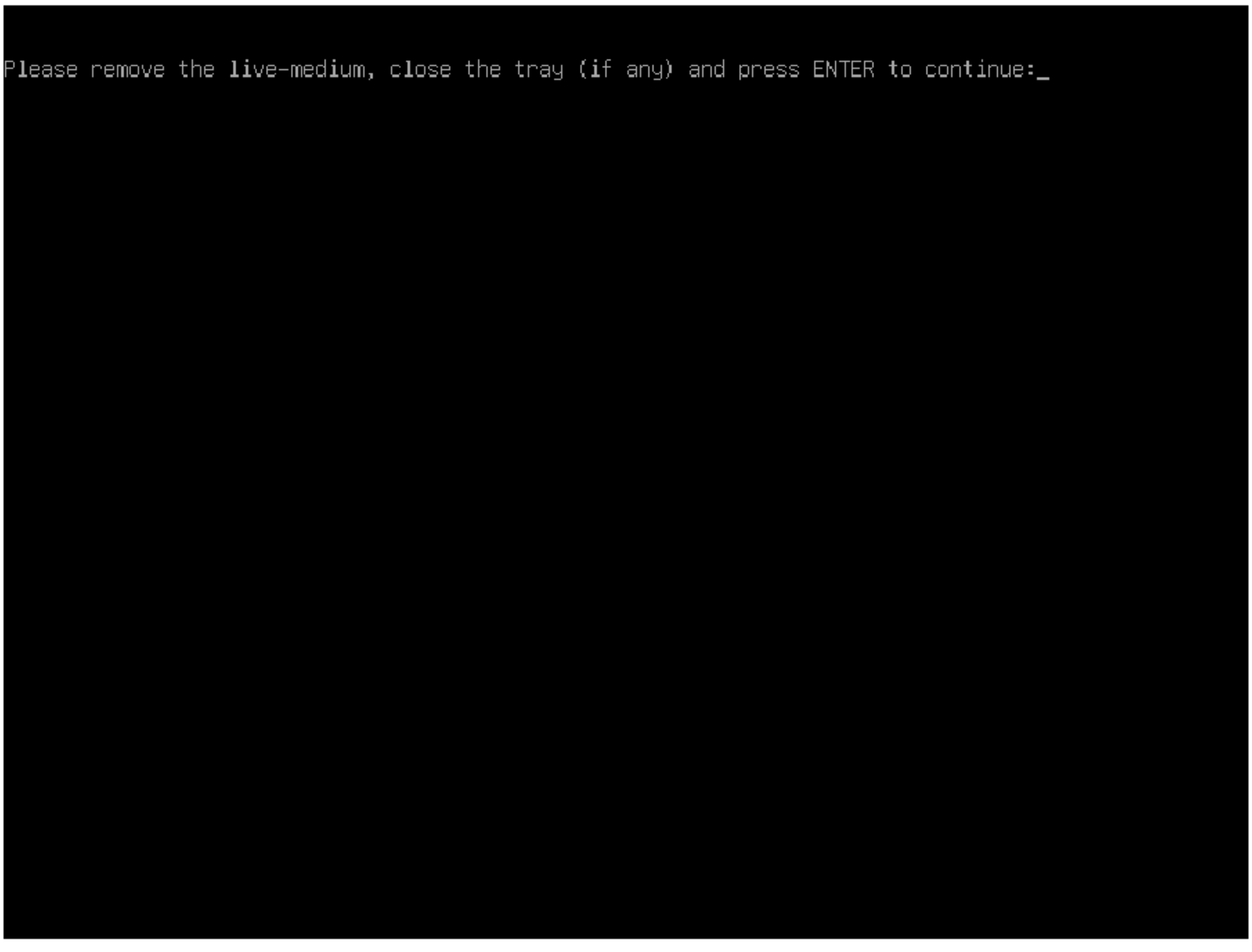
At this point the restoration will be carried out:



To the point of announcing that it is ready for a reboot:

```
n grub-install later.
Found boot loader grub in the MBR of disk /dev/sda.
There is a separate boot partition in target device. Trying to mount root partition for grub-install
 to work with that...
Setting up the Logical Volume Manager
  2 logical volume(s) in volume group "debian-vg" now active
/dev/mapper/debian--vg-root is mounted as root partition for grub-install...
Found grub 2 installed in the restored OS.
Test if we can chroot the restored OS partition /dev/mapper/debian--vg-root...
Yes, we are able to chroot the restored OS partition /dev/mapper/debian--vg-root.
Trying to use the grub2 in the restored OS...
Running: run_grub2_from_restored_os "/dev/sda1" "/dev/mapper/debian--vg-root" "/dev/sda"
Re-installing grub2 on disk/partition /dev/sda with grub2 dir in partition /dev/sda1 and root partit
ion /dev/mapper/debian--vg-root...
The options for grub2-install in the chroot: --force --recheck --no-floppy  /dev/sda
Installing for i386-pc platform.
Installation finished. No error reported.
done!
**************************************************.
Running: run_ntfsreloc_part -p "sda1 sda5" auto
The NTFS boot partition was not found or not among the restored partition(s). Skip running partclone
.ntfsfixboot.
**************************************************.
End of restoreparts job for image 2017-01-18-11-img.
End of restoredisk job for image 2017-01-18-11-img.
**************************************************
**************************************************
Checking if udevd rules have to be restored...
This program is not started by Clonezilla server, so skip notifying it the job is done.
Finished!
Now syncing - flush filesystem buffers...
Ending /usr/sbin/ocs-sr at 2017-01-18 13:25:48 UTC...
"ocs-live-general" finished.
Check /var/log/clonezilla.log for more details.
The next step: reboot
Trying to unmount /home/partimag... done!
Will reboot (Press Ctrl-C to abort)... 7 6 5 4 3 _
```

Finally, press enter to allow the reboot (since clonezilla was started over the network, no disk needs to be removed):



8.5.5 Miscellaneous Notes

Clonezilla user/password management

The `clonezilla` user is created by `fuss-server create` which generates a random password and saves it in `/root/clonezilla_cred.txt` and adds it to the `sshaccess` group.

With `fuss-server upgrade`, the user's presence and membership in the group is verified (and restored if necessary). For the password, if the file `/root/clonezilla_cred.txt` is not present a new one is generated and set.

If you want to change passwords for the `clonezilla` user you can simply use `passwd`, but it is your responsibility to update `/root/clonezilla_cred.txt` with the new password.

8.6 Installations in schools in the Autonomous Province of Bolzano.

The standard installation procedure in schools in the Autonomous Province of Bozen includes *Installing Proxmox on Debian*, followed by *Installing fuss-server on Proxmox* following the specific cautions in this section.

8.6.1 Installation of Debian

During installation remember to:

- Make a note of the name of the network cards, especially WAN;
- Give the machine a host name following established standards (e.g., `galilei-prox`);

- follow the standards even to choose the domain name (e.g. `galilei.blz`);
- choose a local user name (e.g. `local-fuss`, with password `local-fuss`);
- Enter DNS servers 208.67.222.222 and 208.67.220.220;
- Delete any pre-existing partitions.

For disk partitioning, two cases can arise: if the server "s native RAID is not recognized (as is the case, for example, with Fujitsu TX 1320 M1 or 2 Servers and HP Proliant Microserver Gen8), it is ne- cessary to follow the procedure for *Installing Debian on Software RAID*; otherwise, you can proceed directly with the guide for *Installing Proxmox on Debian*, using the following partitioning scheme:

mount	dimensions	partition type	filesystem
/boot	1 GB	*Physical* partition	ext4 with journaling
/ (root)	50 GB (max)	LVM logic volume	ext4 with journaling
swap	4 GB	LVM logic volume	swap
/var	50+ GB	LVM logic volume	ext4 with journaling

8.6.2 Additional configuration of Debian

Once the installation and network configuration is complete, it is a good time to install some additional useful programs.

If you want to install the microcode package for intel processors, you need to enable the non-free-firmware repositories in `/etc/apt/sources.list`:

```
deb http://ftp.it.debian.org/debian/ bookworm main contrib non-free-firmware
deb-src http://ftp.it.debian.org/debian/ bookworm main contrib non-free-firmware

deb http://security.debian.org/debian-security bookworm/updates main contrib non-.
↪free-firmware
deb-src http://security.debian.org/debian-security bookworm/updates main contrib␣
↪non-free-firmware

# bookworm-updates, formerly known as 'volatile'
deb http://ftp.it.debian.org/debian/ bookworm-updates main contrib non-free-
↪firmware
deb-src http://ftp.it.debian.org/debian/ bookworm-updates main contrib non-free-.
↪firmware
```

Then install the desired programs:

```
# apt update
# apt install vim gedit net-tools dnsutils molly-guard hyperf screen
etherwake # apt install intel-microcode
```

Note: For example, the intel-microcode package is needed in case the error `TSC_DEADLINE disabled due to Errata...` appears when starting Proxmox.

For more information, see the related thread on the proxmox forum

---

8.6.3 Proxmox Installation

Problems with DELL PowerEdge T630 servers.

If you experience problems booting with the proxmox kernel installed above (which can happen with kernel 4.15.18.1, for example) reboot the system and, in the GRUB screen, select Advanced / `Advanced` mode and then boot with an older kernel.

At this point you can search for which kernel corresponds to the most recent proxmox ISO, at https://www.proxmox.com/en/downloads follow the link to the iso information and then the link to the release notes.

Instructions to be completed after update to the current state of support for the server in question

Problems with HP servers

With some HP servers and some RAID controllers (HWRaid HP P222 P222i P420 or P420i) data corruptions occur when the IOMMU is activated, which happens by default for kernels after version 5.15-23. You can check which controllers are present with the command:

```
lspci | grep -i raid
```

are listed as possibly problematic those mentioned and the Gen8 Smart Array.

To remedy the problem, you must disable the feature by passing `intel_iommu=off` as the kernel boot option; for this you must edit `/etc/default/grub`, adding the above option to the definition of the `GRUB_CMDLINE_LINUX_DEFAULT` variable with:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet intel_iommu=off"
```

and apply the changes by running `update-grub`.

Problems reaching the interface of Proxmox

In case the proxmox web interface does not respond, check in `/var/log/daemon.log` if an error such as:

```
Apr 13 16:18:24 prox1 pveproxy[3535]: /etc/pve/local/pve-ssl.key: failed to load␣
↪local private key (key_file or key) at /usr/share/perl5/PVE/APIServer/AnyEvent.
↪pm line 1642.
```

In the case, use the following commands to correct:

```
# systemctl restart pve-cluster
# pvecm updatecerts
```

followed by a reboot of the machine

Proxmox Update

In the event that you need to upgrade Proxmox to a later version, you can se- guate the project guides, choosing the appropriate one for your case at https://pve.proxmox.com/wiki/Category: Upgrade

8.6.4 Installation of fuss-server

When installing the fuss-server, the goal is to create a VM that can be transported to another Proxmox host, and thus be compatible with the hardware characteristics of the smallest server in the entire fleet.

Partitioning scheme

The recommended partitioning scheme is:

swap	max 8 GB	same amount as the RAM
/	50 GB	
/var	min 100 GB	
/srv	min 100 GB	Hosts Clonezilla software and images Calibrate size by number and size of the images you want to use
/ho-me	rhyme-nente	

Remembering to use LVM and that enlarging partitions is easier than shrinking them, so if you leave some space free it is better to underestimate the size needed and possibly enlarge it in the future.

Configuration of network interfaces

An example of `/etc/network/interfaces` suitable for fuss-server is as follows:

```
# The loopback network interface
car lo
iface lo inet loopback

# The primary network interface -- WAN
auto eth0
iface eth0 inet static
        address 192.168.94.3
        netmask 255.255.255.0
        192.168.94.0 network
        broadcast 192.168.94.255
        192.168.94.1 gateway

# The secondary network interface - LAN
auto eth1
iface eth1 inet static
        address 192.168.0.1
        netmask 255.255.255.0
        192.168.0.0 network
        broadcast 192.168.0.255
```

In case you want to use a captive portal you will need to configure a third network interface.

8.6.5 Saving and restoring images

Before configuring the fuss-server with `fuss-server create` you can create a complete dump of the VM, transportable to other Proxmox hosts.

In this way, to create the FUSS server for other schools, one can start from an almost completed machine on which network/user-specific features can be arranged and the configuration completed.

Dump

Note: The device on which the dump is being done must not contain pre-existing dumps of a VM with the same ID as the one we are operating on.

If so, you can group the directories related to the pre-existing dump (`dumps`, `images`, `private`, `templates`) into a new directory, e.g., `old_dumps`.

1. Mounting external storage

   Connect the external HD to the server (possibly to a USB 3 port) and make sure Proxmox mounts the device (just click it in *File Manager*).

   Check the point of mount, which will be type `/media/<logged_user_name>/.<label_hd_exterior>`.

2. Unplug the fuss-server ISO from the virtual machine DVD.

   Click on VM, on Hardaware, double-click on CD/DVD Drive and choose "Do not use any media"; confirm.

3. Add the external disk to available storage.

   - Click on Datacenter, then on Storage, and then on Add.
   - Choose Directory
   - Give a name (ID:) to the storage, such as `BACKUP SERVER`.
   - Enter the mount point of the external disk in the Directory field.

4. Effect the dump.

   - Make sure the virtual machine is turned off.
   - Expand the Content drop-down menu, click on VZDump backup file and then the light blue Add button.
   - Click on the VM, on Backup, and then on Backup now.
   - In the Storage menu select the one you just added.
   - In the Mode menu, select snapshot.
   - Leave the LZO (fast) compression type selected.
   - Click on the light blue Backup button.

   The process will create a file named `vzdump-quemu.....lzo` in the disk `dump` directory outside.

5. Disconnect the external disk.

   - Click on Datacenter, Storage, on the row corresponding to the external disk, then on Remove and confirm with Yes.
   - Disassemble the disk from the Proxmox host.

Restore

In case you already have a dump of FUSS Server, when you have reached the end of the *Installation of Proxmox on Debian you* can restore it.

Warning: The target host will need to be configured with a bridge scheme identical to that of the host on which the snapshot was created.

- On the destination server, copy the dump `.lzo` file to the `/var/lib/vz/dump/` directory.
- From the terminal, perform the restore operation:

```
# cd /var/lib/vz/dump/
# qmrestore <file_dump>.lzo <id_machine>.
```

where <machine_id> (e.g. 100) is different from any other machines on the proxmox server.

At this point it is necessary to adapt the virtual machine to the new school.

- in Options change the name of the virtual machine.
- In Hardware delete and recreate Network Interfaces.
- Adjust the quatity of RAM and the number of CPUs if necessary.

Then, at the first boot of the virtual machine, change the following parameters:

- root password
- machine hostname in /etc/hosts and /etc/hostname
- network addresses in /etc/network/interfaces.

CHAPTER 9

Bug reporting

9.1 Collection of information

When something goes wrong, it may be necessary to report a bug (*Report*) on the appropriate project at https://work.fuss.bz.it/; before doing so, it is important to gather all relevant information to help diagnose the problem.

9.1.1 version numbers

Rather than indicating "updated as of date X," better to indicate the precise version numbers of the package(s) you suspect may be involved in the problem, obtaining them with, for example:

```
dpkg -l <package name>
```

9.1.2 `fuss-server` and `fuss-client`

For diagnosis, it is important to record all messages provided by ansible during installation, so report everything printed by the command from the beginning.

If you are in the console (physical or of a virtual machine) you can save all the output of the command by using the script command beforehand, for example:

```
script
<command>
...
exit # to be given when the command ends
```

where `<command>` will from time to time be `fuss-server create`, `fuss-client -a` or their various variants; this saves all output to the `typescript` file in the current directory.

CHAPTER 10

Policies

This section documents the policies adopted in schools adopting FUSS, with information on their implementations.

10.1 Authentication specifications

With version 7.x of the fuss-server, authentication credential management criteria were introduced to be compliant with current requirements dictated by privacy regulations, particularly regarding the complexity and expiration of passwords.

Only lecturers are subject to these requirements (since students do not process other people's data). Therefore, a specific value of the multivalue attribute *operational unit*, `ou` (assignable to each user) was used to distinguish students and faculty. In particular, this should be set according to the following table:

Lecturers	`ou=doctors`
Students	`ou=students`

The password management system with system commands was set up using the following line of in /etc/pam.d/common-password:

```
required pam_cracklib.so retry=3 minlen=8 difok=3 minclass=3
```

implying minimum length of eight characters, no repetition of more than three characters in the password change, presence of at least three among the four classes of characters: upper case, lower case, numbers, punctuation.

The web application for changing passwords allows you to avoid these restrictions but applies only to users who have attribute `ou=students`.

For password expiration this is set when creating an LDAP user by setting a value in days in the `ShadowMax` attribute of the user, the same value is applied. The defaults set by the FUSS server configuration do not include password expiration, as this is not necessary for most users (which are students). In particular this is not set if you use the `smbldap-tools` package commands. If you need to intervene manually you must use the `chage.py` script installed like the others under `/usr/share/fuss-server/scripts/`, specifying a value in days with the `-M` option.

10.1.1 Octofuss

Octofuss automatically sets the value of `ou=` corresponding to a user, based on the groups to which that user belongs. If the user is put in a secondary group called "`lecturer`" or "`teachers`," he gets the `ou=docents`. If he is not in these groups, then he gets the `ou=students`.

At the same time, for teachers, a password expiration value of 90 days is automatically set, as required by privacy regulations. For students, on the other hand, a default of 99999 days is used, implying that it will not expire.

10.2 Internet access

The Internet access policies set by fuss-server are:

- Unauthenticated users are not allowed to browse, with the exception of the various software repositories that are authorized for ease of installation, listed in the ACL `repository` inside `/etc/squid3/squid.conf`, plus those that may have been added (functionality available since version 8.0.38 of fuss server) in `/etc/squid3/squid-added-repo.conf`.
- Authenticated users exit only if they are part of the `internet` (local) group of the fuss-server (permission `Internet` inside Octonet).
- In the proxy configuration, it is possible to restrict access to the Internet network during restricted hours Monday through Friday from 7 a.m. to 10 p.m. and Saturdays from 7 a.m. to 2 p.m. To achieve this restriction, the Squid configuration must be modified by replacing the line in `/etc/squid3/squid.conf`:

```
http_access allow password internet
```

  with the line:

```
http_access allow password internet time
```

- Accesses to Internet sites are recorded in the system log files.
- Internet browsing is done in protected mode (using the Dansguar- dian/E2guardian content filter). As of fuss-server version 8.0.38 this restriction is disabled by default on the local network since there is already a filter upstream of the schools' network, you can rehabilitate the use of the filter by changing the `dans_exclude_localnet` variable in *fuss-server-defaults* `.yaml` (see *Fuss Server Defaults File*).
- `Internet` access is by default blocked for Windows machines; you can re-enable it by changing the `proxy_win_exclude` variable in `fuss-server-defaults.yaml` (see *file-default-fuss-server*).

10.2.1 Checks

It is important to perform all the indicated checks to be sure that the proxy really works.

- try browsing with an authorized user (i.e., entered in the `Internet` group) by correctly indicating username and password;
- Trying to navigate with an authorized user by correctly stating username but getting the password wrong;
- Try browsing with an unauthorized user (i.e., not entered in the `Internet` group) by correctly indicating username and password;
- try browsing with an authorized user using his correct credentials, then try removing him from the `Internet` group and see if the proxy blocks him.

Keep in mind that removal or addition to the `Internet` group does not take immediate effect. If this vie- ne done through Octonet or `octofussctl` in fact the permission must be propagated by `octofuss-client`

which can take up to 5 minutes, in addition Squid helpers need to see the new permissions (until they finish the previous value is seen), and the `nscd` cache needs to be refreshed.

Therefore, if you want to be sure that the permission is propagated right away you need (starting with version 8.0.42 of `fuss-server`) to restart the `propagate-net-perm` service (also available among the services that can be restarted from the Octonet interface).

For earlier versions, the equivalent commands are:

```
octofuss-client --dryrun
nscd -i group
systemctl stop squid3
systemctl start squid3
```

10.2.2 FTP

To enable FTP traffic, it is necessary to allow traffic of this service through the firewall (unblock port 21/tcp).

CHAPTER 11

11.1 Update fuss-server via dump and restore

Beginning with versions 8.0.48 and 10.0.28 of fuss-server, the necessary tools and a procedure to dump a FUSS8 server and restore it to a FUSS10 server have been prepared to enable the transition from FUSS 8 to FUSS 10 while retaining much of the data on the source server.

11.2 Dumping operations on the original server (FUSS8).

The procedure is to make a full backup of the users' homes on the server (which must include in addition to `/home` any other directories in which these may have been placed), from which to then restore the data. It will be assumed that this was done with the `fuss-backup program` and that restoration of the `/homes` is done with this program (restoration of the home data can be done at a later time).

The first step in the procedure is to run the script `/usr/share/fuss-server/scripts/fuss-dump.sh` on the source server (assumed to be a FUSS 8), this will create a file `fuss-server-dump-$DATA.tgz` in the current directory with the data needed for the restore, which will need to be copied to the new server at its destination (t h e archive data will still remain saved on the original server under `/var/backups/fuss-dump`).

11.3 Operations on the new server (FUSS10)

It will then be necessary to install the operating system on the new server, and to configure its network; it is advisable to use the same hostname as on the previous server; changing it could in fact give rise to inconveniences related to names remaining in the cache on clients, so it is better to keep the same hostname. Also, if disk quotas are being used on the old server, they will need to be enabled on the new one as well.

Warning: The dump procedure and the restore procedure assume that quotas are active on at most one filesystem, as normal on a fuss-server, this is obtained from `/etc/fstab` by looking for the `usrquota` and `grpquota` mount options, which must be active on only one filesystem (need not be the same between original and new machine).

In order to use the recovery, you must install the new FUSS10 server normally, with `fuss-server created`, but keep the domain, master password, and workgroup identical. You should also keep the same internal network and DHCP range, since some data (especially firewall settings and static reservations) may depend on these settings.

Therefore, before running `fuss-server create it` is a good idea to copy the data from the starting server configuration (the file `/etc/fuss-server/fuss-server.yaml`, which is also in- cluded in the archive produced by the dump script as `fuss-server.yaml.old` anyway) and edit only the `external_ifaces:` and `internal_ifaces:` entries, which can be changed (as is the case when switching from Jessie to Buster), adapting them to the new server in case it is necessary.

You can still extract the data from the dump which is a simple tar compressed with:

```
tar -xvzf fuss-server-dump-$DATA.tgz
```

and the previous fuss server configuration file will be in `fuss-dump/fuss-server.yaml.old`.

Once you have completed the basic configuration of the fuss-server you will need to copy the file with the data dump to it, and run the restore script with:

```
/usr/share/fuss-server/scripts/fuss-restore.sh fuss-server-dump-$DATA.tgz
```

the script once unpacked the archive in the `fuss-dump` subdirectory (it will overwrite any files of the same name it contains) will stop all services, reimport the data, and then restart them.

Since NFS/Kerberos data may be affected by caching by the server (which runs in the kernel) it may be appropriate to restart the server after performing the restore.

At this point the users and service configurations will have been reimported, but it will remain to restore the contents of the users' homes, an operation to be done with the instructions given for using `fuss-backup`.

Warning: The new server, having been reinstalled, will have different SSH keys than the old one, so connecting from clients may result in errors of not recognizing the server's SSH fingerprints due to this change. It will be necessary to delete the old keys and accept the fingerprints of the new keys (be sure to mark them when reinstalling).

As a final note, starting with version 8.0.50 (and 10.0.34) of fuss-server the file with the configuration defaults (`/etc/fuss-server/fuss-server-defaults.yaml`) will not be included in the dump, but simply copied alongside `fuss-server.yaml.old` (as `fuss-server-defaults.yaml.old`) in the `fuss-dump` direc- tory, this is because in the development of Fuss 10 some additional confi- gurations variables were added that were not present with Fuss 8, the lack of which would cause `fuss-server` to fail on a run after reset. For this reason, the file is still saved so that any changes made from the default installed by the package can be checked, and reapplied.

Warning: Keep in mind that the removal of `fuss-server-defaults.yaml` from the totally reprised files only occurs if you run `fuss-dump.sh` in the version installed with a fuss-server later the 8.0.50, this should always be true if you have kept your machines up to date as a good practice, if this has not happened, the file will still be present and will overwrite the new one installed with `fuss-server create`. If you are not sure save the file before performing the restore.

This section includes guides on various topics of utility in schools related to installations for particular hardware.

12.1 PC with special requirements

12.1.1 PC HP ProOne 440 G6 24 All-in-One

For the 'audio operation of the HP ProOne 440 G6 24 All-in-One machines, the firmware-signed package must be installed:

```
apt update
apt install firmware-sof-signed
```

At this point the audio from the built-in webcam still does not work and the following procedure should be followed.

1) The arecord -l command allows you to locate card and microphone device (in the 'example below 0.7):

```
root@aulamuse:~# arecord -l
**** List of CAPTURE Hardware Devices ****
card 0: sofhdadsp [sof-hda-dsp], device 0: HDA Analog (*) []
  Subdevices: 1/1
  Subdevice #0: subdevice #0
card 0: sofhdadsp [sof-hda-dsp], device 1: HDA Digital (*) []
  Subdevices: 1/1
  Subdevice #0: subdevice #0
card 0: sofhdadsp [sof-hda-dsp], device 6: DMIC (*) []
  Subdevices: 1/1
  Subdevice #0: subdevice #0
card 0: sofhdadsp [sof-hda-dsp], device 7: DMIC16kHz (*) []
  Subdevices: 1/1
  Subdevice #0: subdevice #0
```

2) In /etc/xdg/autostart create a file alsamodule.desktop that contains:

```
[Desktop Entry]
Version=1.0
Type=Application
Name=alsamodule
Comment=Load module to use embedded webcam audio; the device
↪may vary and is inferred from the command "arecord -l"
Exec=/bin/sh -c 'sleep 1;/usr/bin/pacmd "load-module module-alsa-source
↪device=hw:0.7"'
Terminal=false
StartupNotify=true
```

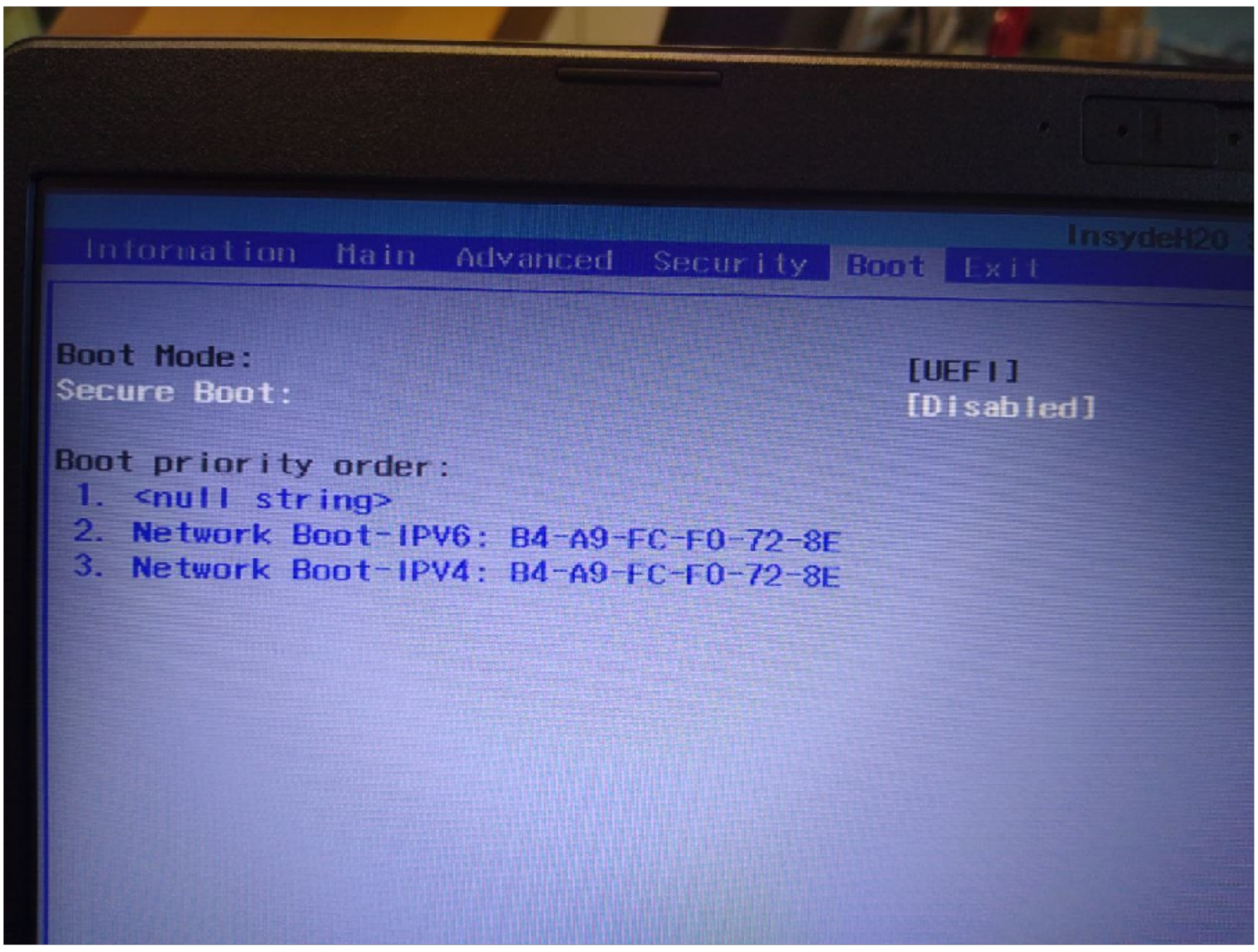
3) After restarting, clicking on the Pulseaudio icon will provide one more item, `Entry`, which allows you to select the built-in device.

12.2 Notebooks with special requirements

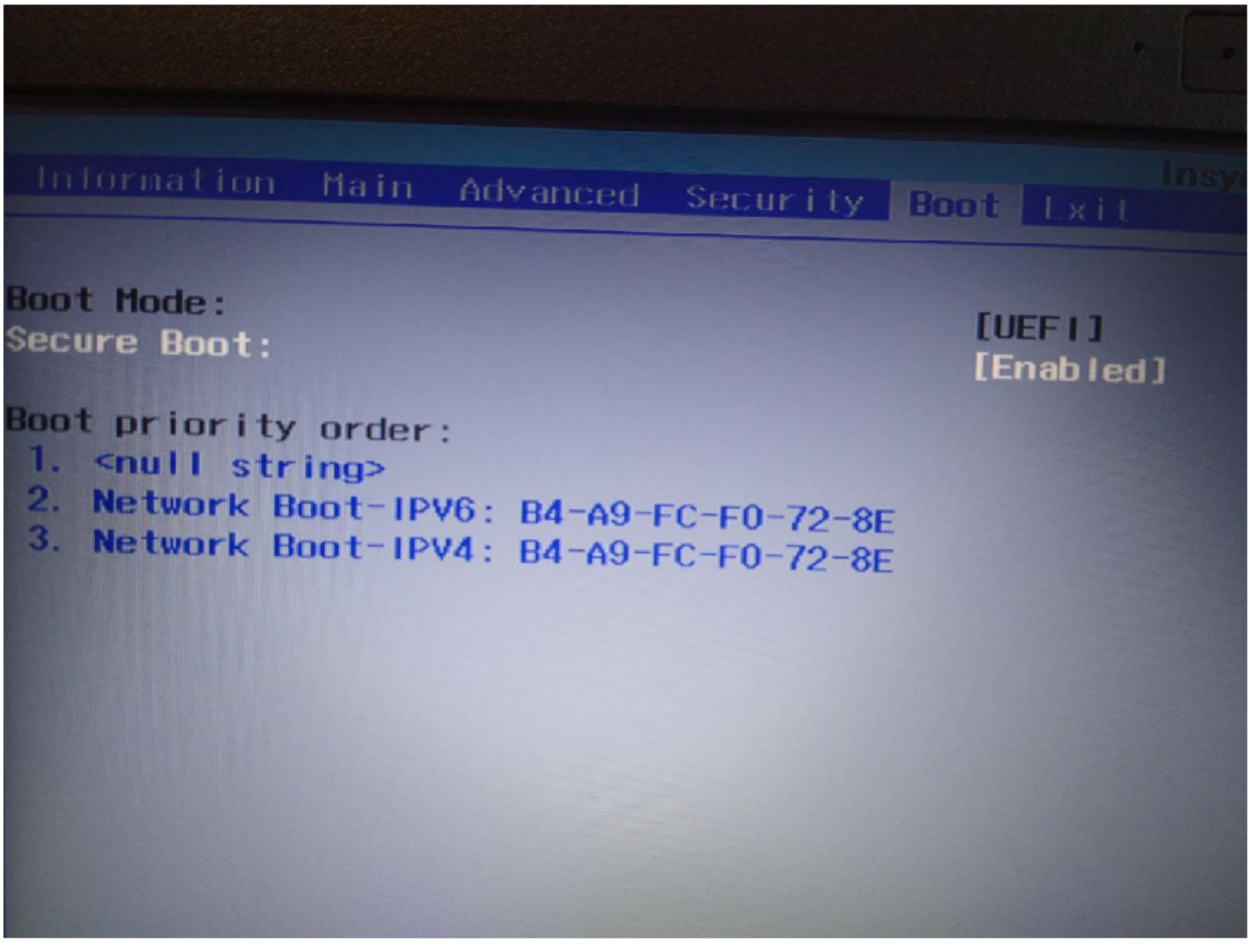
12.2.1 Acer TravelMate TMP-214 Notebook

Image installation using Clonezilla

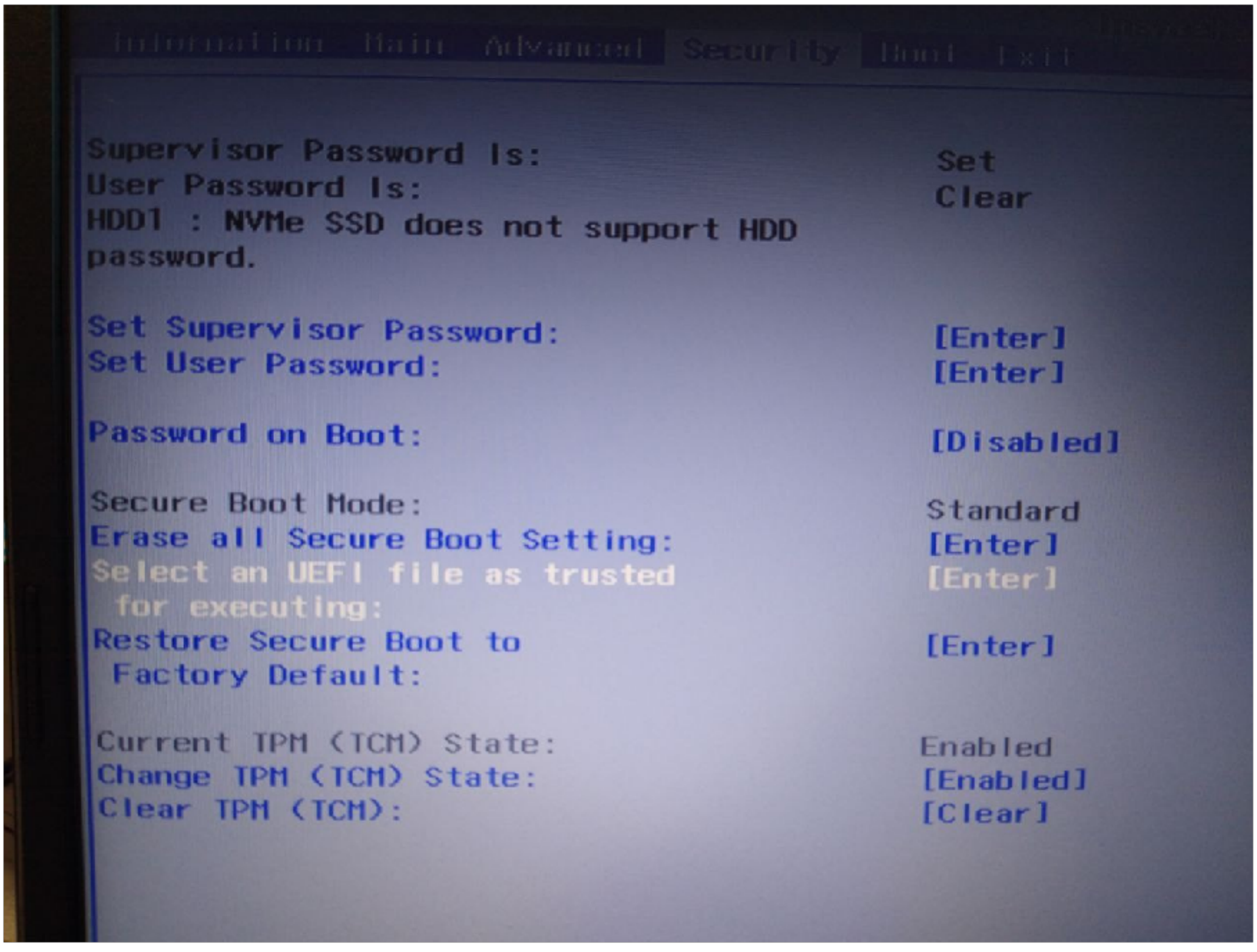
Before installing a FUSS image via Clonezilla (via PXE boot or USB stick) you need to access the notebook setup menu with *F2*. Under the *Security* tab, first set the Supervisor password by pressing *Enter* on *Set Supervisor Password*. Then disable the *Secure Boot* item in the *Boot* tab as shown in the following image:

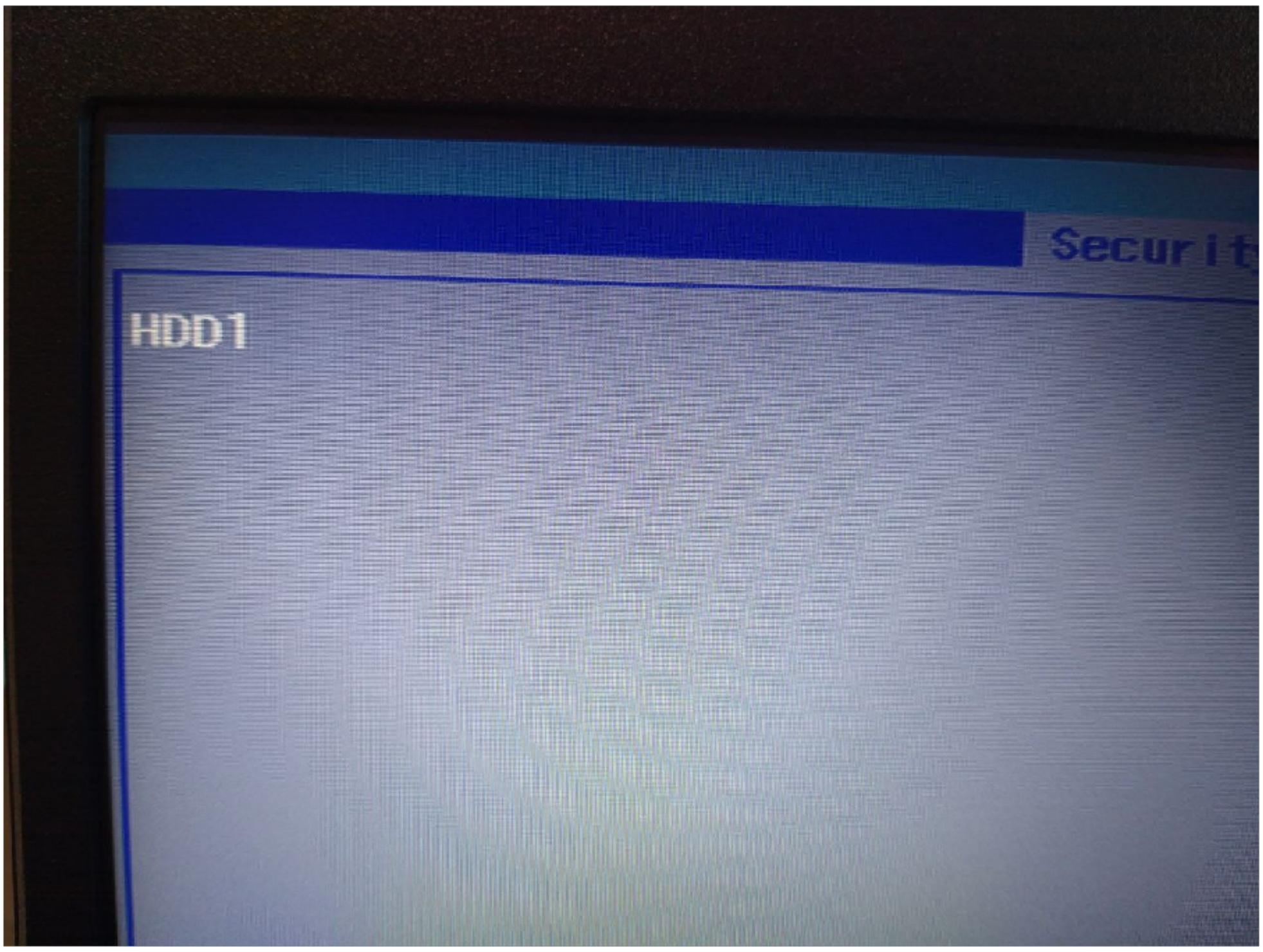


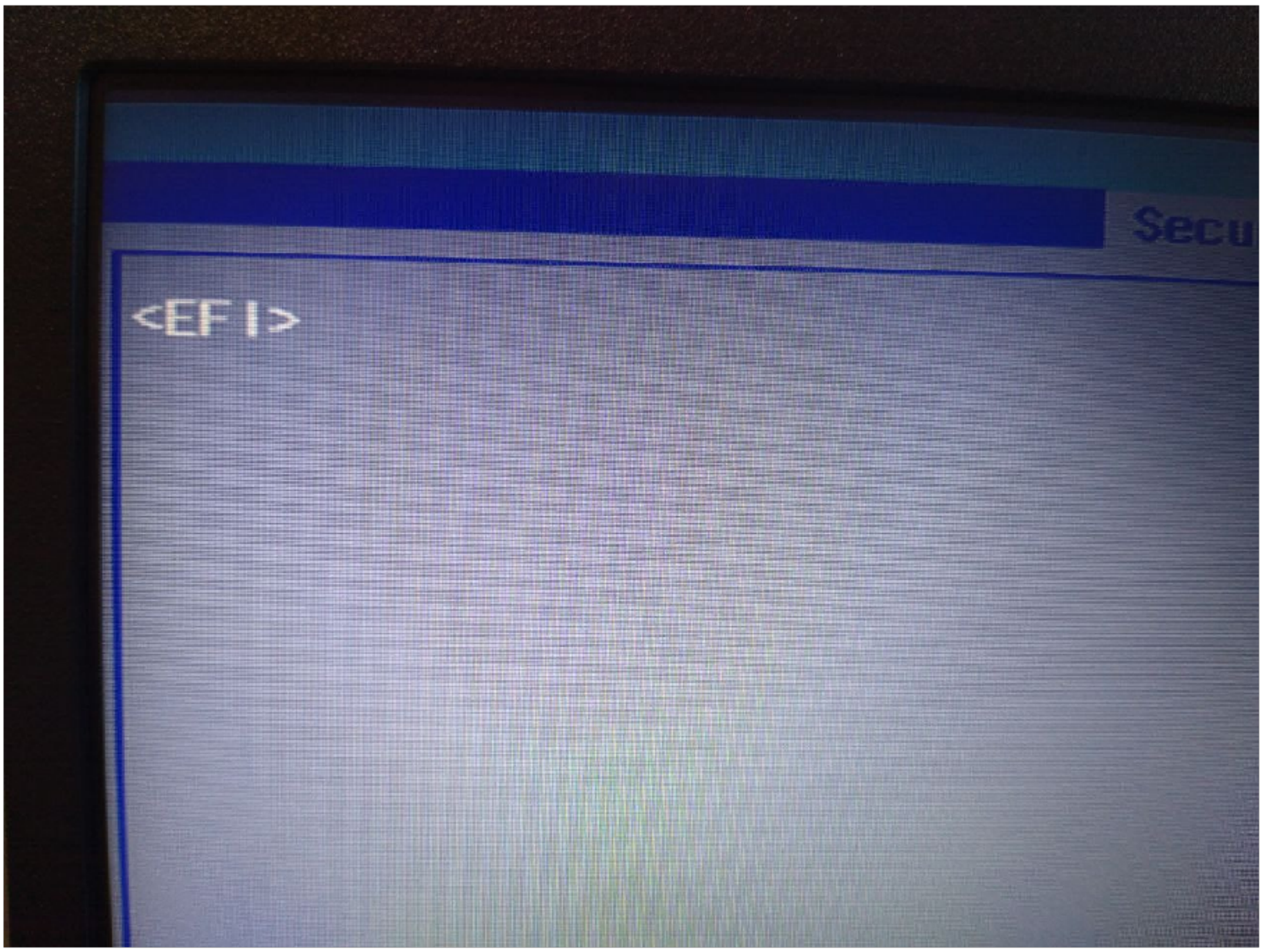
After cloning the FUSS image and restarting the notebook, re-enter setup with *F2*, re-enabling *Secure Boot*.

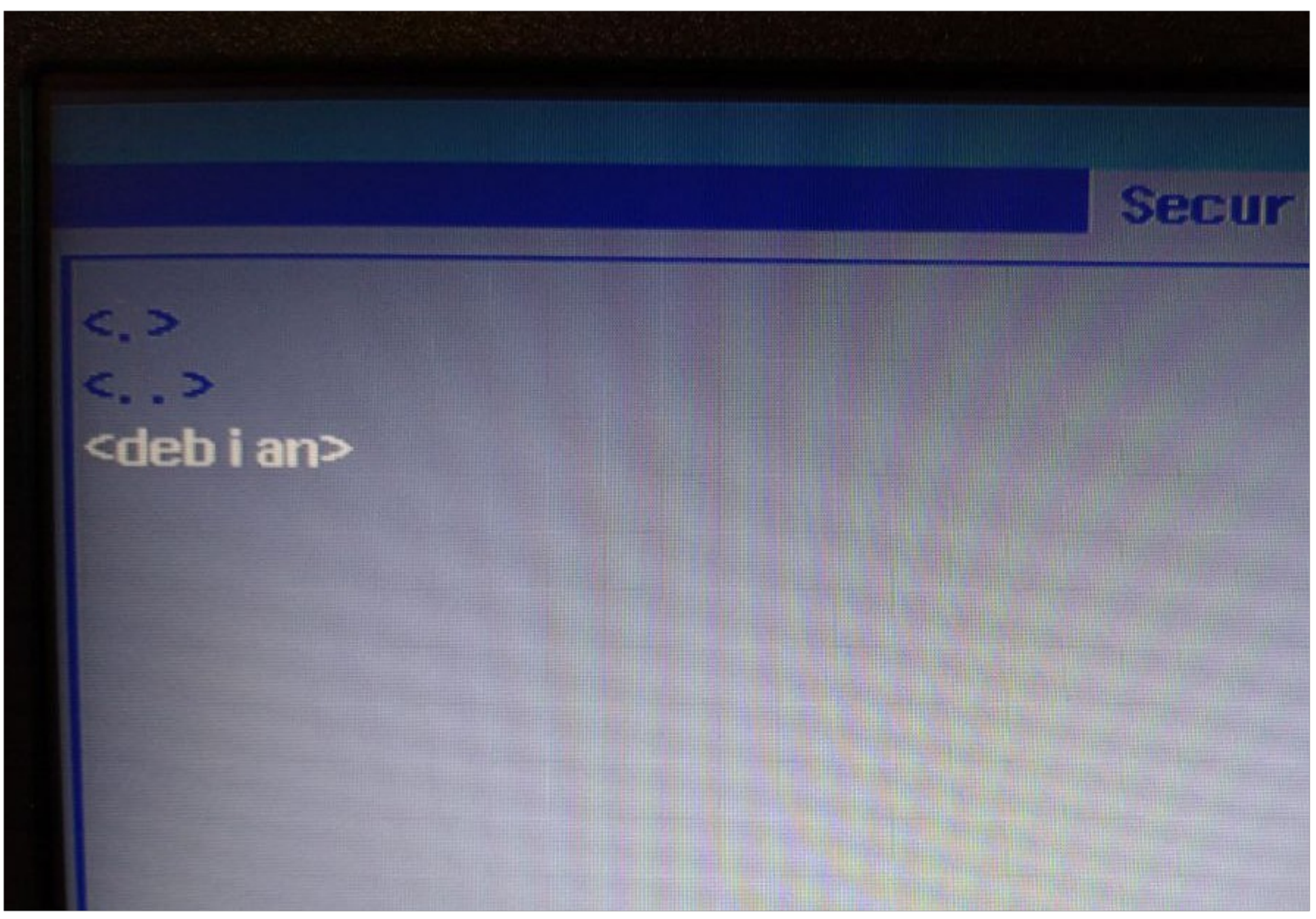


Select the item *Select an UEFI file as trusted for executing* by going through the folders of the HDD1 disk: `<EFI> -> <debian>`.

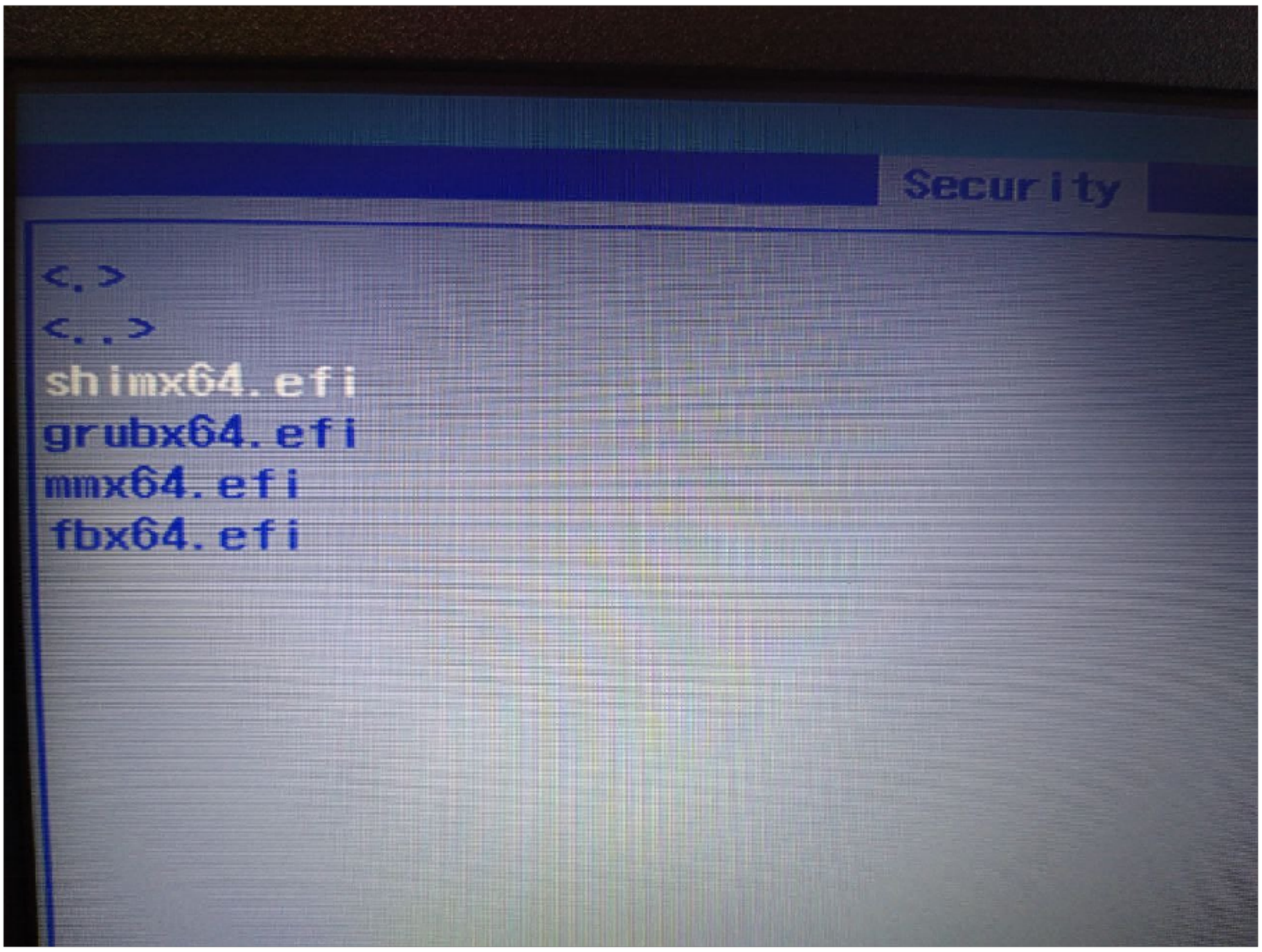

Information Main Advanced Security Boot Exit
Supervisor Password Is: Set
User Password Is: Clear
HDD1 : NVMe SSD does not support HDD password.
Set Supervisor Password: [Enter]
Set User Password: [Enter]
Password on Boot: [Disabled]
Secure Boot Mode: Standard
Erase all Secure Boot Setting: [Enter]
Select an UEFI file as trusted for executing: [Enter]
Restore Secure Boot to Factory Default: [Enter]
Current TPM (TCM) State: Enabled
Change TPM (TCM) State: [Enabled]
Clear TPM (TCM): [Clear]

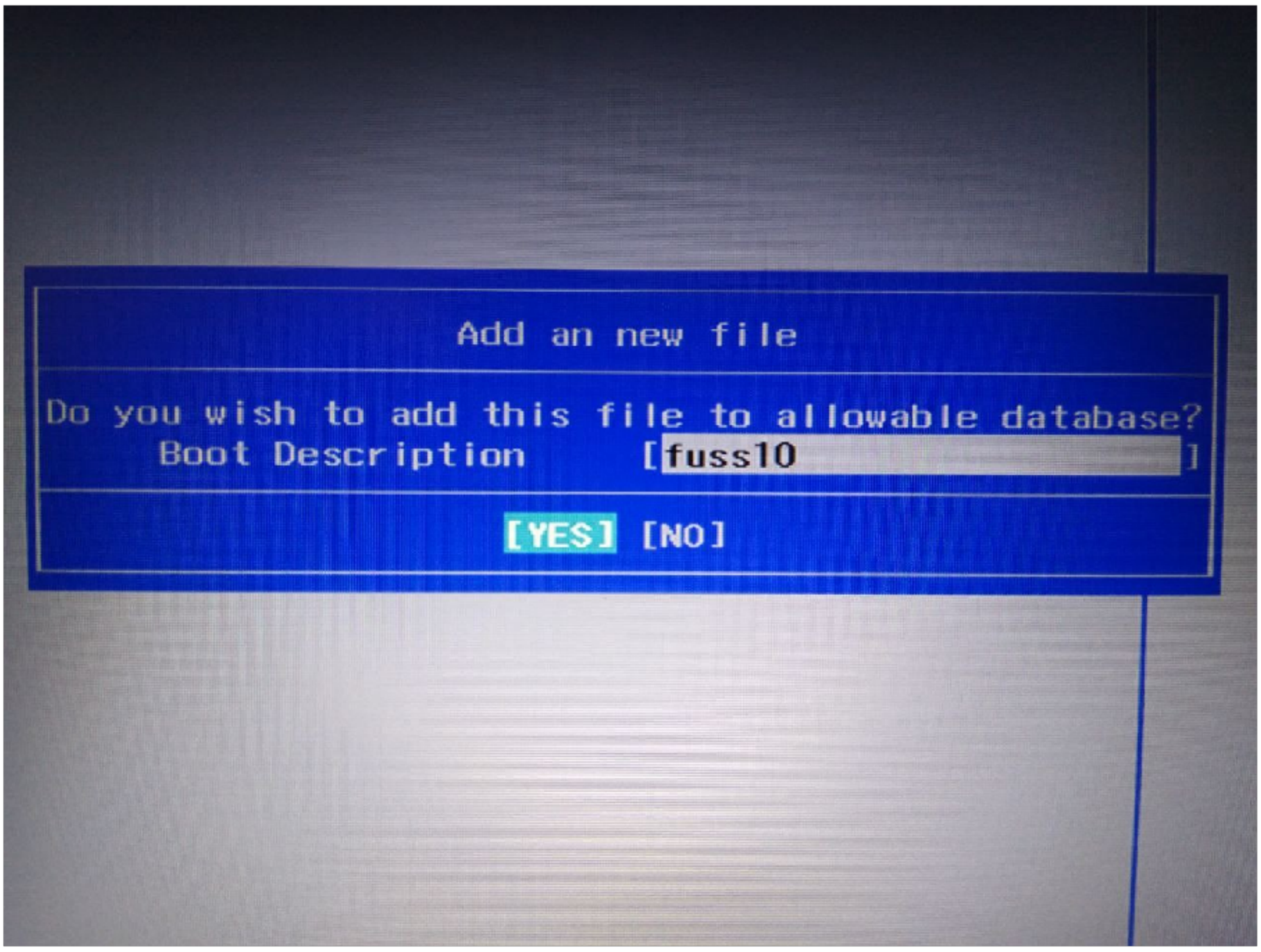

Securit
HDD1


Secu
<EFI>

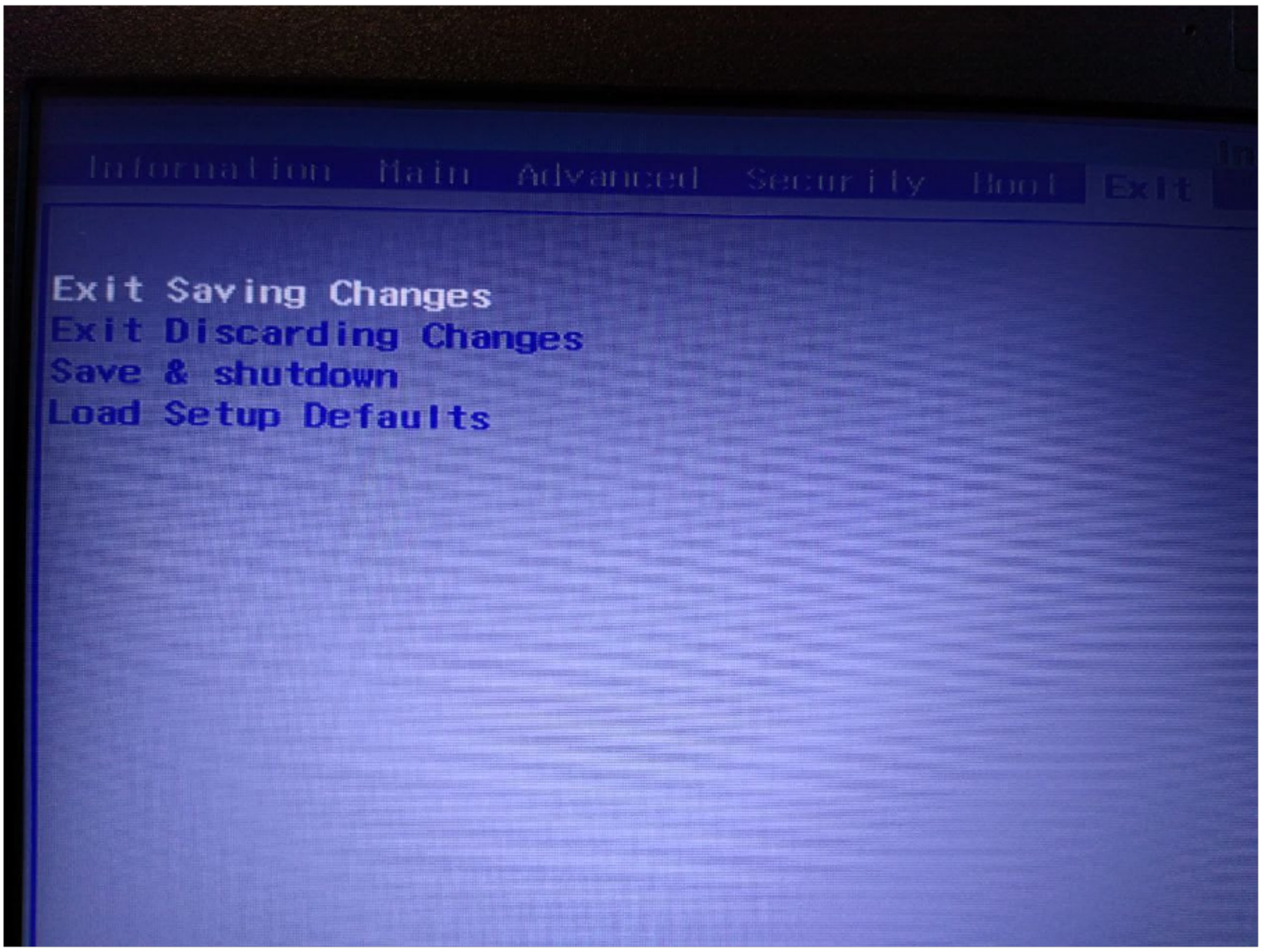

Secur
<.>
<. . >
<deb i an>

You choose the `shimx64.efi` file by pressing *Enter* and entering the description of this boot option in the pop-up, e.g., `fuss10` confirming with *Yes*.





When finished, save the changes by pressing *Exit Saving Changes* in the *Exit* tab or simply pressing *F10* confirming on completion.



12.2.2 HP ProBook 430 G5 Notebook

Wifi

For wifi operation, see:

wireless-HP ProBook

12.2.3 HP ProBook 450 G5 Notebook

Wireless

For wifi operation, the `firmware-realtek` package must be installed if not already present. Perform:

```
apt update
apt install -t stretch-backports linux-image-amd64 firmware-realtek
```

Video

The laptops (HP ProBook 450 G5) have `1920x1080` as the only resolution.

The following code adds the resolutions of the projector (or other video output device) to the laptop (`eDP-1` interface) and thus makes it possible to **mirror the screens** .

```
for i in $(xrandr | awk '{print $1}' | grep "x")
do
if [ "$i" != "1920x1080" ]; then
xrandr --addmode eDP-1 $i
fi
done
```

The code should be added to script `/etc/fuss-client/display-setup-script/ setDisplayResolution` which will therefore become:

```
#!/bin/sh

for i in $(xrandr | awk '{print $1}' | grep "x")
do
if [ "$i" != "1920x1080" ]; then
xrandr --addmode eDP-1 $i
fi
done

HOSTNAME=$(/usr/bin/hostname)
autorandr --load $HOSTNAME || autorandr common || true
```

Once the projector resolutions have been added, the second part of the script allows au- tomatic mirroring of the two devices already in the login window. The scripts placed in `/etc/fuss-client/ display-setup-scripts` are in fact launched when lightdm is started.

12.2.4 HP UEFI boot - no bootable device

Introduction

In some recent HP models, bootable only with UEFI, after installing the Fuss10 image the boot fails and at boot time a message appears like:

```
NO BOOTABLE DEVICE
```

The problem is due to the fact that UEFI cannot find the EFI file automatically. One solution may be the following:

1) Restart the machine and press the key for manual boot (usually F9)
2) Choose `Boot from file` and then:
   - > PciRoot . . . > EFI > debian > grubx64.efi # if Secure Boot is disabled.
   - > PciRoot . . . > EFI > debian > shimx64.efi # if Secure Boot is enabled.
3) After the system starts up, open a terminal session and launch:

   ```
   efibootmgr
   ```

   The previous command lists the available startup options and startup order, as in the following example

```
BootCurrent: 0001
Timeout: 0 seconds
BootOrder:
Boot0000* Fuss10    HD(2,c8800,82000,a0d91f49-899b-46ac-8863-
↪35f2d16774c4)File(\EFI\debian\grubx64.efi)
Boot0001* Fuss10    HD(2,c8800,82000,a0d91f49-899b-46ac-8863-
↪35f2d16774c4)File(\EFI\debian\shimx64.efi)
Boot2001* USB Drive (UEFI) RC
Boot2002* Internal CD/DVD ROM Drive (UEFI) RC
```

4) At this point you should locate the menu item you entered with, e.g., `Boot0001`

5) Set or change the boot order with the command

```
efibootmgr -o 0001.0000
```

where `0001` are the 4 digits following "Boot"; it is not necessary to enter all the entries, the first one is sufficient.

6) In case you want to display the menu at startup, simply lengthen the `Timeout` to 5 seconds or more with:

```
efibootmgr -t 5
```

7) Reboot the machine and verify that the system starts up

12.2.5 Lenovo IdeaPad 120s Notebook

Introduction

Such a notebook does not have an RJ45 socket, so a USB-RJ45 adapter is required to connect to the network. Such an adapter is not recognized by the BIOS to allow a *network* boot and allow booting a Clonezilla image from a FUSS server. "It is necessary to have a USB stick to which a Clonezilla image must be copied in advance.

BIOS changes

First, it is necessary to change the BIOS settings. After turning on the notebook, press the *F2* key to access the BIOS (Phoenix SecureCore Technology Setup). Under the *Security* item make sure that *Secure Boot* is *Disabled*. Under the *Boot* heading change *Boot Mode* to *Legacy Support*. Exit by saving the changes with *F10*. The notebook will be rebooted.

Starting Clonezilla

After inserting a bootable USB flash drive with a Clonezilla image (the version used for this guide is 2.5.6-22), for the choice of boot device, press *F12* and select *USB HDD*.

After startup, Clonezilla will ask you to select the interface language and possibly change the keyboard layout from the default one. After this first setting, the *Start Clonezilla* window will be shown in which the eponymous item should be selected.

This is followed by the *device-image* option, *ssh_server* and *dhcp*. The notebook will receive an IP address from the FUSS server, and immediately after that you will need to enter the IP address of the server (e.g. `192.168.0.1`), the port (typically `22`), the user account (`clonezilla`), the folder on the server where Clonezilla should read the image (typically `/srv/ clonezilla`), and the `clonezilla` user's password.

After entering the password, Clonezilla will ask for the execution mode: choose *Beginner* and then *restoredi- sk*; the images available on the server will be shown. Choose a 64bit FUSS 9 image (less than 64 GB in size) that you will have previously uploaded to the FUSS server in the `/srv/clonezilla` folder. Confirm the destination disk on your notebook (`mmcblk1`) by pressing *Enter*. Choose whether or not to do an image check before the restore and finally choose the action to perform when finished (*choose*, *reboot* or *poweroff*). Press *Enter* and confirm with *y* twice. Clonezilla will copy the image indicating the time required to finish the operation.

wireless-HP ProBook

12.2.6 Lenovo ThinkPad P15 G2

For audio configuration (output and input) see: *HP ProOne 440 G6 24 All-in-One PC*

12.3 Management and installation of printers and scanners

Printers in a FUSS network are managed through OctoNet, as described in the *Network Printers* section Of the related guide.

This section describes the installation procedures for some printer models that have been recently manufactured and for which the installation procedure includes additional steps.

12.3.1 HP PageWide Pro 452dw

From the list of HP printers posted at https://developers.hp.com/hp-linux-imaging-and-printing/supported_devices/index we see that this printer needs a version of the `hplip` (HP Linux Imaging and Printing) package at least equal to `3.16.3`.

The version of `hplip` present on the FUSS server (Debian 8 "Jessie") is `3.14.16` which does not provide for this printer model. Therefore, it is necessary to install `hplip` in version `3.16.11` found in the `jessie-backports` repository, which must first be included in the `/etc/apt/sources.list` file:

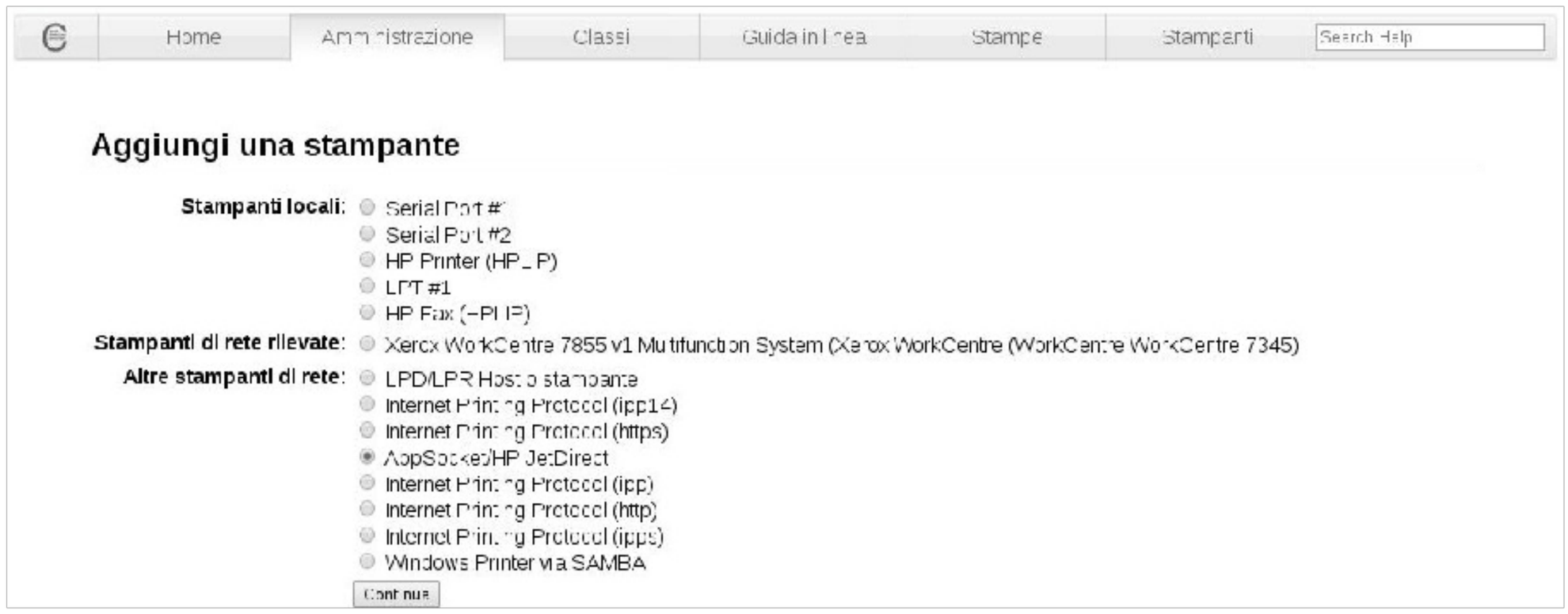
```
deb http://httpredir.debian.org/debian jessie-backports main contrib
```

Update server packages and install hplip from jessie-backports:

```
apt update
apt -t jessie-backports install hplip
```

After connecting to the server via ssh in X11 Forwarding mode with `ssh -X NOMESERVER`), we open `firefox` by connecting to the URL http://localhost:631 to which the CUPS web interface responds.

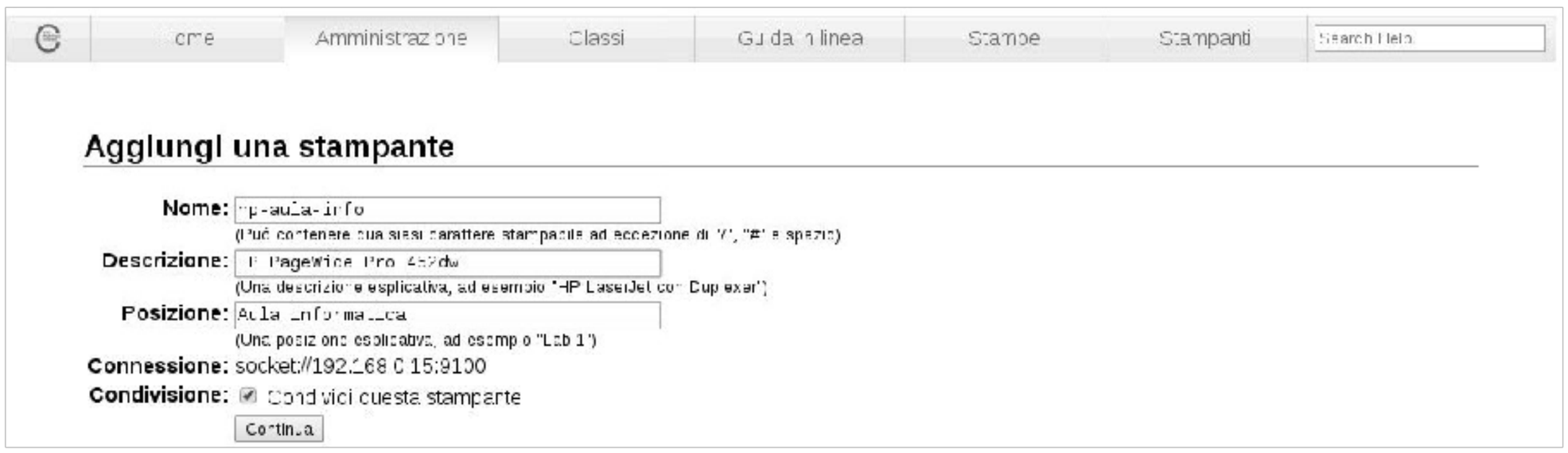
Choose *Administration - Add a Printer*, following the steps as shown in the following screenshots. First choose the AppSocket/HP JetDirect option and then press the *Continue* button.



Indicate in the connection field `socket://IP_STAMPLE:9100` after assigning the printer a static IP.



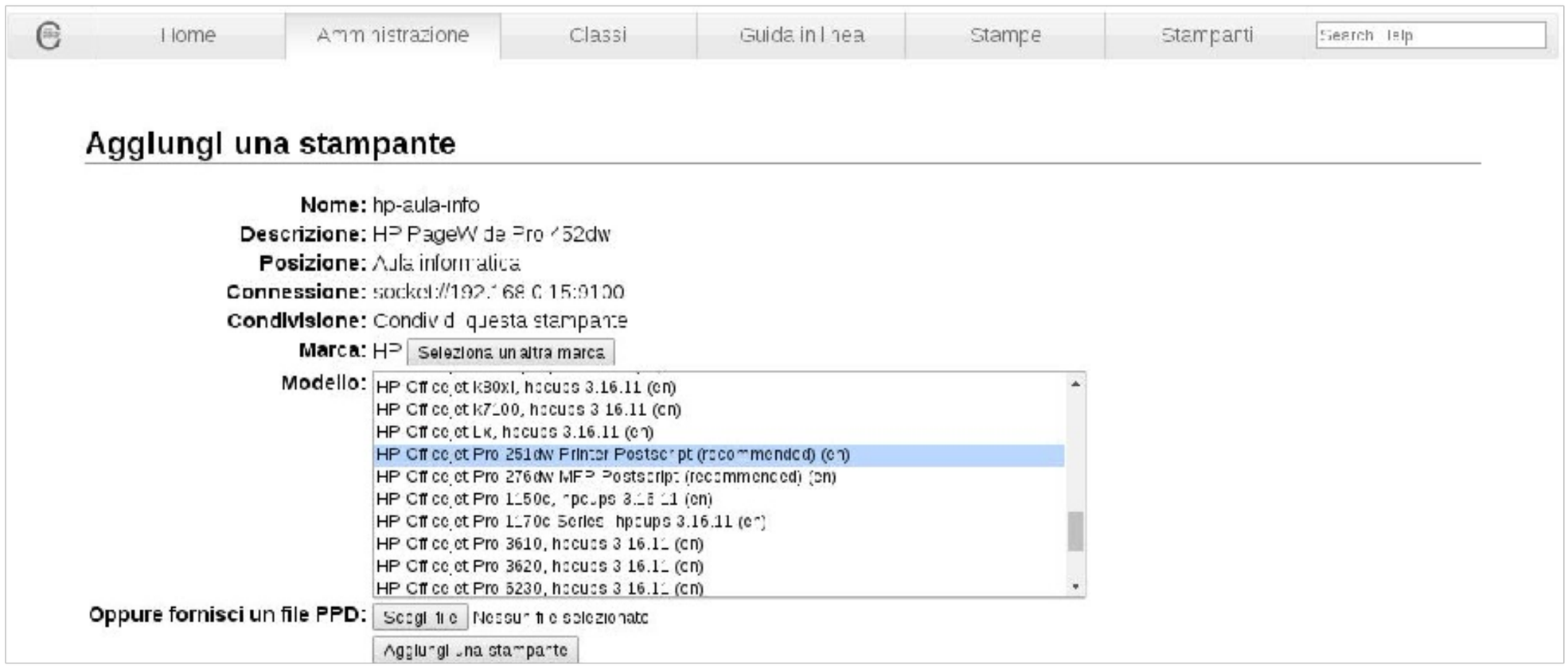
Enter the *Name*, *Description* and *Location of* the printer on the next screen and adding the sharing flag.



Choose the brand of the printer (Make)



And then follow with the model. Let *HP Officejet Pro 251dw* be chosen, which is the name of the compatible model suggested by HPLIP.



Check that the *Media size* is correctly set to *A4* size



and finally, by selecting the *Installed Options* item, indicate that *Tray 2* is installed and press the *Set Default Options* button.



Now the printer is correctly configured. The last step remains, which is to enable clients to print, an operation that must be done in OctoNet as described in the dedicated section.

12.3.2 Brother MFC-L6900DW

Download the two necessary DEB packages (`mfcl6900dwcupswrapper-3.5.1-1.deb` and `mfcl6900dwlpr-3.5.1-1.deb` at the following link:

http://fuss.bz.it/utility/printers/Brother_MFC-L6900DW

Install them with:

```
dpkg -i mfcl6900dw*
```

After connecting to the server via ssh in X11 Forwarding mode with `ssh -X NOMESERVER`), we open `firefox` by connecting to the URL http://localhost:631 to which the CUPS web interface responds. Alternatively, we connect via ssh with the server by opening a tunnel with `ssh root@NOMESERVER -L 13631:localhost:631` and open `firefox` in user session by connecting to the URL http://localhost:13631 .

An installation procedure similar to that of the *HP PageWide Pro 452dw* printer is then followed.

Choose `Administration - Add a printer`.

First choose the `AppSocket/HP JetDirect` option and then press the *Continue* button.

Indicate in the connection field `socket://IP_STAMPLE:9100` after assigning the printer a static IP.

Enter the *Name*, *Description* and *Location of* the printer on the next screen and adding the sharing flag.

Choose the brand of the printer (`Brother`).

and following the model: `Brother MFCL6900DW for CUPS .`

Then select the `Installed options` item and confirm by clicking `the Set default options` button.

Finally, enable clients to print, an operation that must be done in `OctoNet` as described in the dedicated section.

12.3.3 Epson Perfection 3490 Scanner

The following tutorial was derived from the link `http://www.autodidacts.io/` how-to-get-epson-perfection-3490-flatbed-scanner-working-on-ubuntu-linux reported and tested by technician Paolo Baratta.

First, you need to install SANE (which stands for Scanner Access Now Easy, a popular back-end for Linux scanners that allows you to use all kinds of different scanners with all kinds of scanning apps. You can install it with the following command:

```
sudo apt-get install sane
```

Create a directory called snapscan in /usr/share/sane

```
sudo mkdir /usr/share/sane/snapscan/.
```

You can download the `Esfw52.bin` firmware by clicking http://cdn.autodidacts.io/misc/Esfw52.bin

or find it elsewhere on the Internet by searching for the file name.

Move the file to /usr/share/sane/snapscan/Esfw52.bin

```
sudo mv ~/Downloaded/Esfw52.bin    /usr/share/sane/snapscan/
```

Change the permissions of the firmware file:

```
sudo chmod 777 /usr/share/sane/snapscan/Esfw52.bin
```

Open the configuration file

```
sudo gedit /etc/sane.d/snapscan.conf
```

Change the top line that says.

```
"firmware /usr/share/sane/snapscan/your-firmwarefile.bin"
```

at

```
"firmware /usr/share/sane/snapscan/Esfw52.bin"
```

Save and exit.

Open /etc/default/saned (which contains the defaults for the saned initialization script) in a text editor:

```
sudo gedit /etc/default/saned
```

And change the line that says `RUN = no` to `RUN = yes`.

Save and exit.

12.3.4 Epson Perfection V370 Photo Scanner

Install the iscan-perfection-v370-bundle-2.30.4.x64 drivers found at the following link: https://download2.ebz.epson.net/iscan/plugin/perfection-v370/deb/x64/iscan-perfection-v370-bundle-2.30.4.x64.deb.tar.gz .

In the unpacked directory is an `install.sh` script that performs the driver installation.

Then follow the procedure given for the Epson Perfection 3490 scanner by replacing the firmware *Esfw52.bin* with the firmware PS1208MFG_FW_ver 1_29.bin that can be downloaded at: https://kb.epson.eu/pf/12/webfiles/Article% 20ZIP%20files/PS1208MFG_FW_ver%201_29.zipper .

12.3.5 Job accounting configuration (process accounting)

Tested with Olivetti dCOPIA 5000MF AND Kyocera TASKALFA 4053ci

The following tutorial allows you to configure PCs so that you can print to printers where Job accounting (process accounting) has been configured.

What should be done on the printer

Job Accounting is a function offered by the above two models and is activated manually, either through the printer's keyboard or from the LAN, or through the printer's Web interface after configuring it with an IP address.

Once the function is activated, accounts (one for each user/department) must be entered, each consisting of a user name and an ID (numeric).

This can possibly be done with a bulk import, via *csv* file (link to file containing specific instructions).

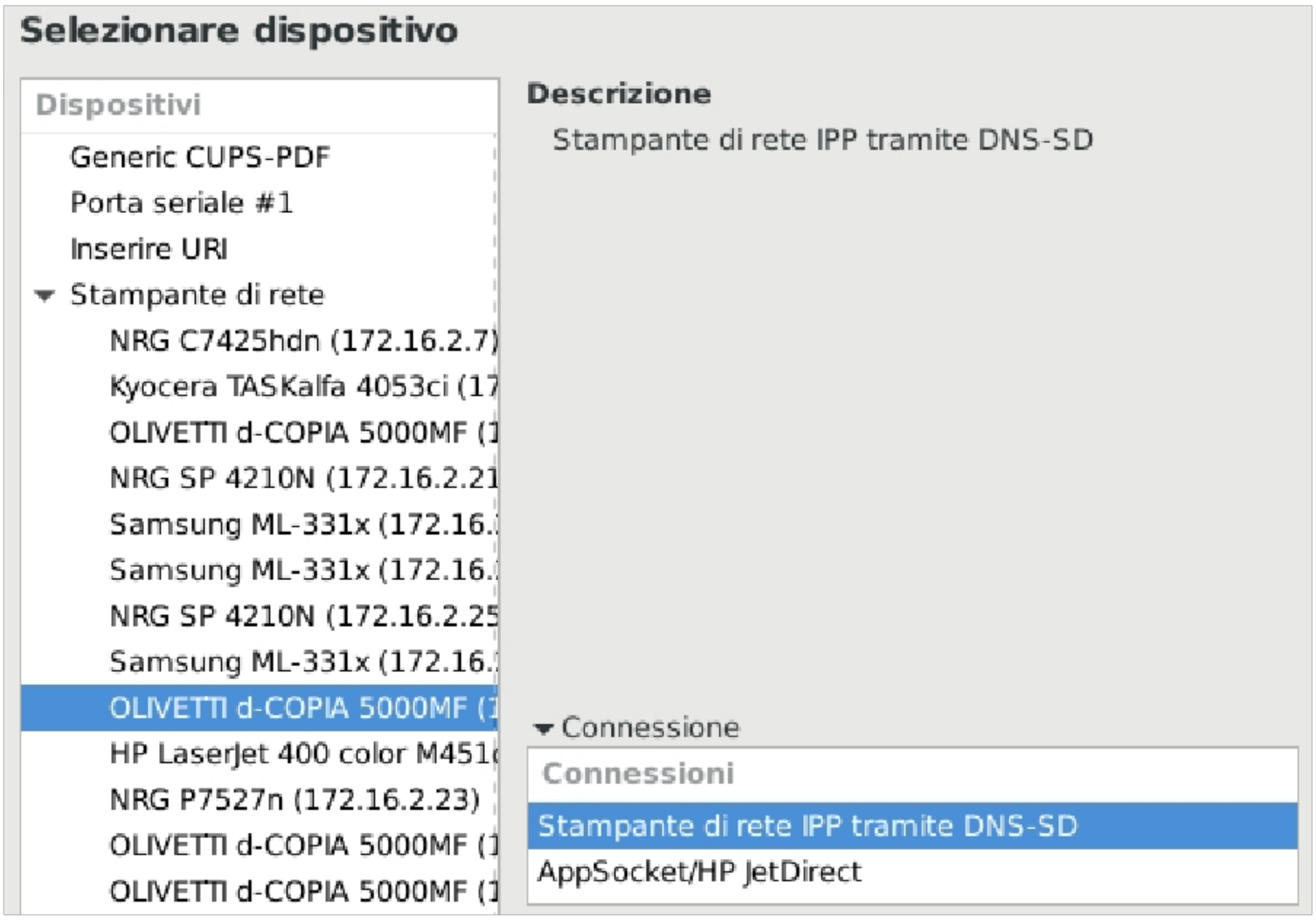
What should be done on PCs

Install the `kyodialog_4.0-1_amd64.deb` package contained in the compressed file (tested version): `Linux_8.7114_TA...xx53ci_x003` found at the following link: https://www.kyoceradocumentsolutions.de/index/serviceworld/downloadcenter.html?initial=false&search=any&searchTerm=Linux&category=driver&language=EN#

Installed the package (deb), among the applications you will find "Kyocera Print Panel"



Install the printer via the "Print Settings" tool (system-config-printer), making sure to select the IPP protocol



- Select the installation mode of choosing PPD and set the one provided at the following link: http://fuss.bz.it/utility/ppd/OLIVETTI-KYOCERA-(KPDL).ppd
- Open CUPS (http://localhost:631), and in the "Printer Management" section, under "Administration," click on the print queue you just created.
- Open the "Administration" drop-down menu, select "Set Default Options," and click on "Job Accounting."
- Open the "Process Accounting" drop-down menu (Job Accounting) and select 000000
- Click on "Set default options" and close CUPS
- Restart CUPS #service cups restart

Personal id setting

The following steps must be performed by each user in order to set their personal id

- Launch the "Kyocera Print Panel tool and select the print queue you want to use.

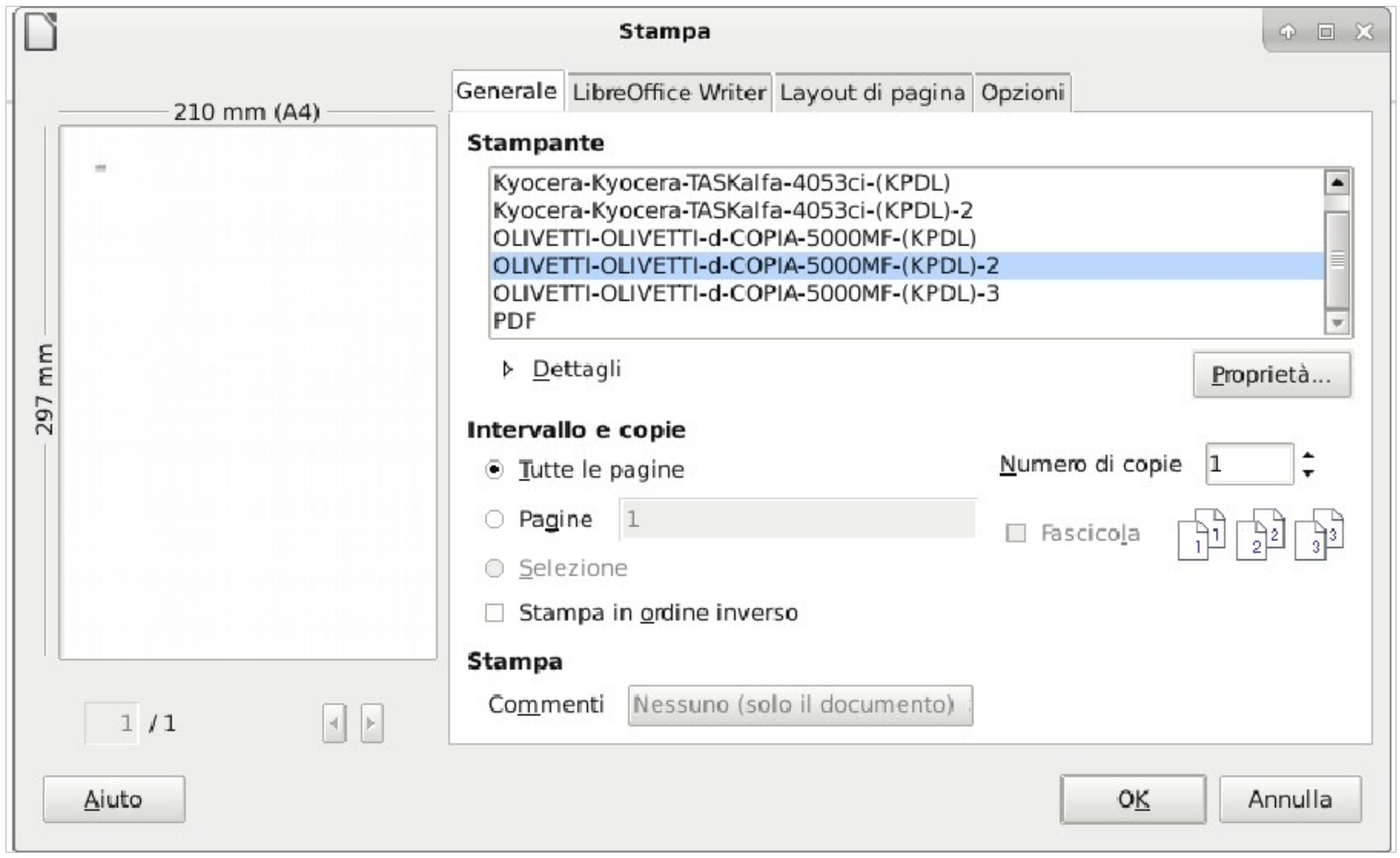
- Click on "Job" (Job) and then check the box corresponding to "Process Accounting" (Job Accounting).
- In the drop-down menu, select "Use specific account ID" and enter your ID.
- Click "OK" and close the "Kyocera Print Panel" tool.

Example of printing using libreoffice writer

- Once the file is produced/opened, click on the printer icon,



- select the print queue and click on "Properties."



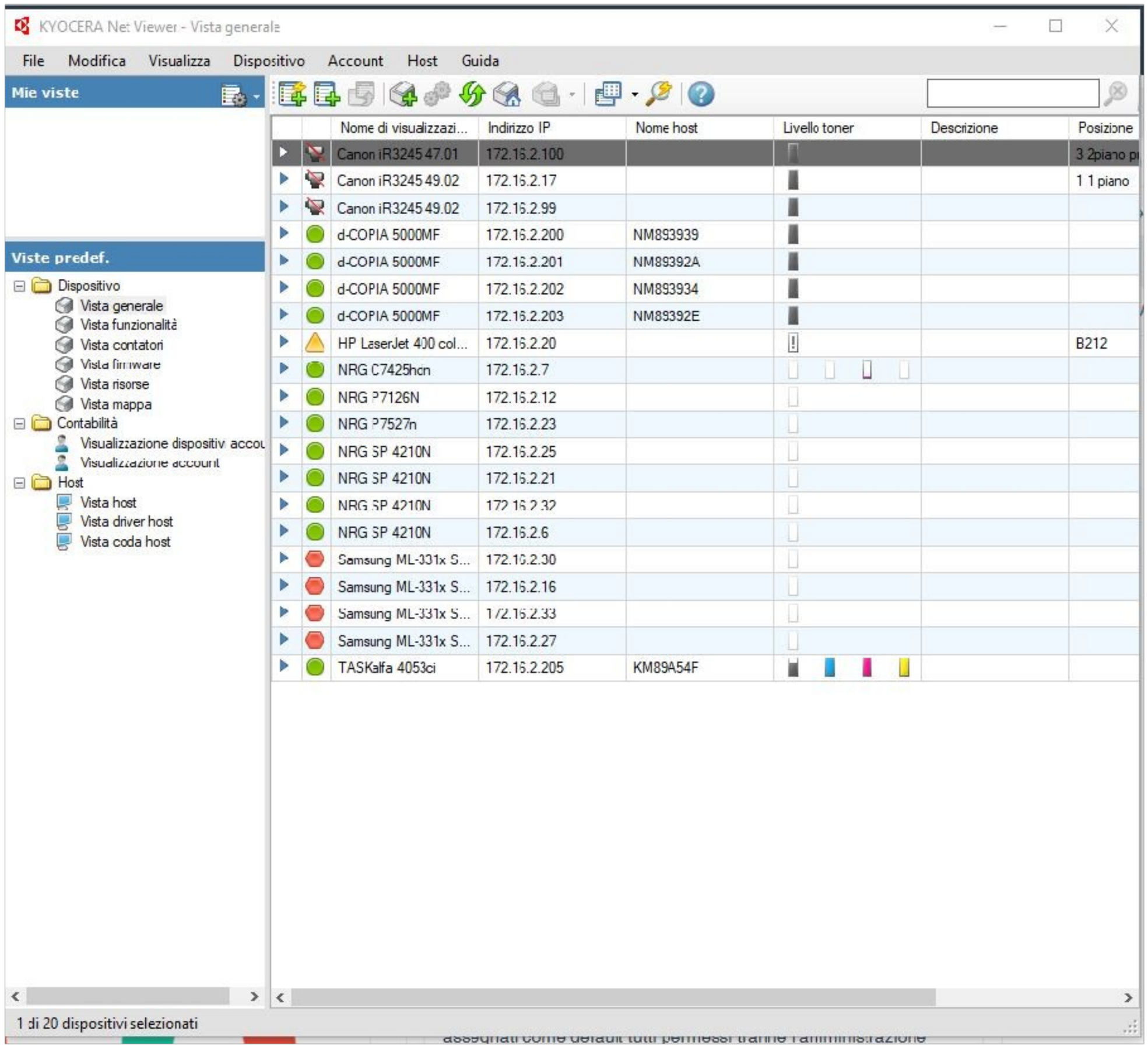
- Open the "Properties" tab, click on "Device" and in the "Option:" menu select "Process Accounting" (Job Accounting)
- In the "Current Value:" menu, select "Custom" (Custom).
- At the top, again under the "Current Value:" menu, a blank field will open in which you should enter your ID.
- Click "OK" twice, and the printout will be sent with the ID code.

12.3.6 Mass account import for Kyocera and Olivetti printers

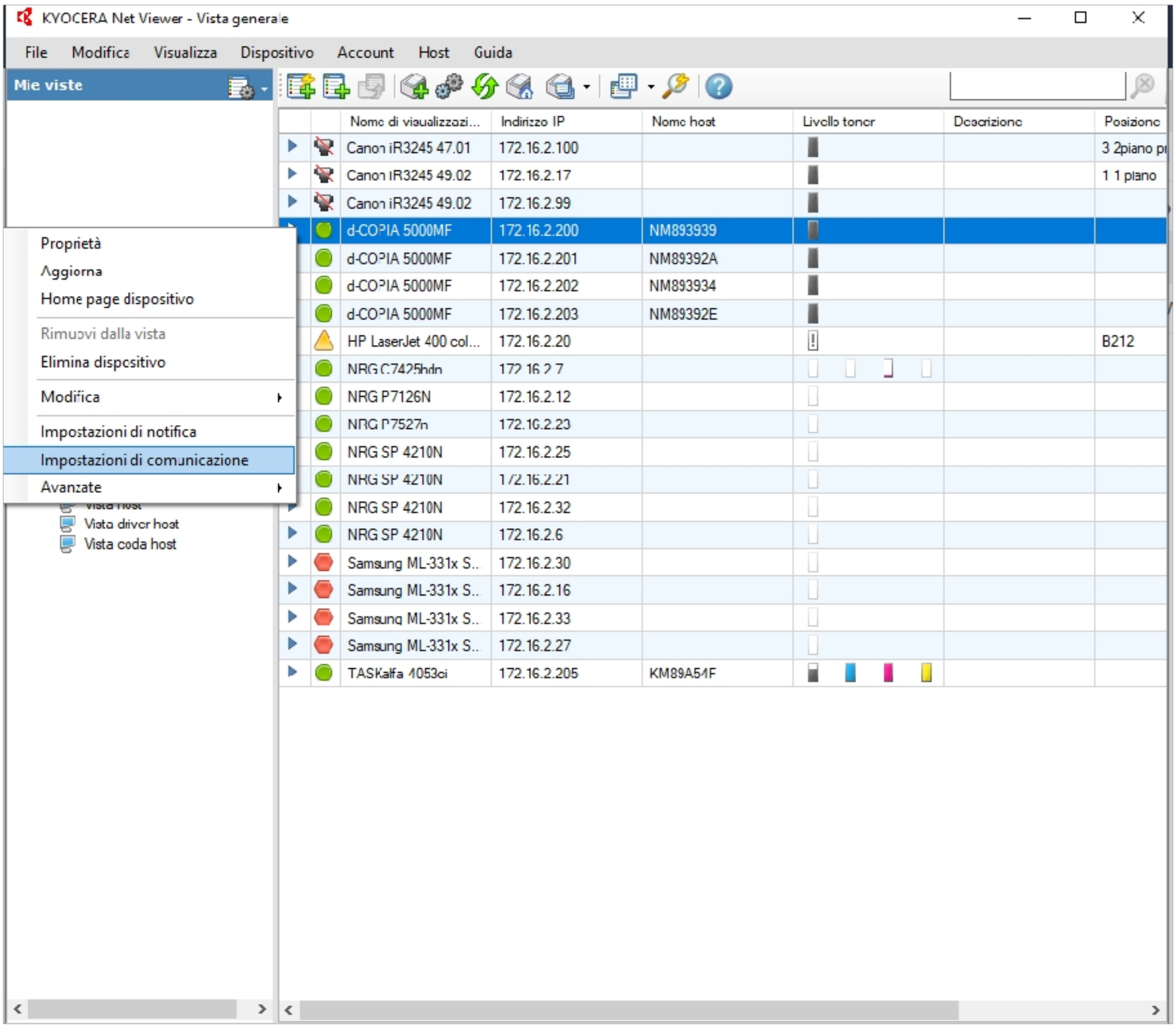
- Install the Kyocera Net Viewer program (KNV package 5.12.1029) in Windows.

  LINK: https://cl.kyoceradocumentsolutions.com/content/dam/kdc/kdag/downloads/technical/executables/utilities/kyoceradocumentsolutions/cl/en/KNV%20v5.12.1029.zipper

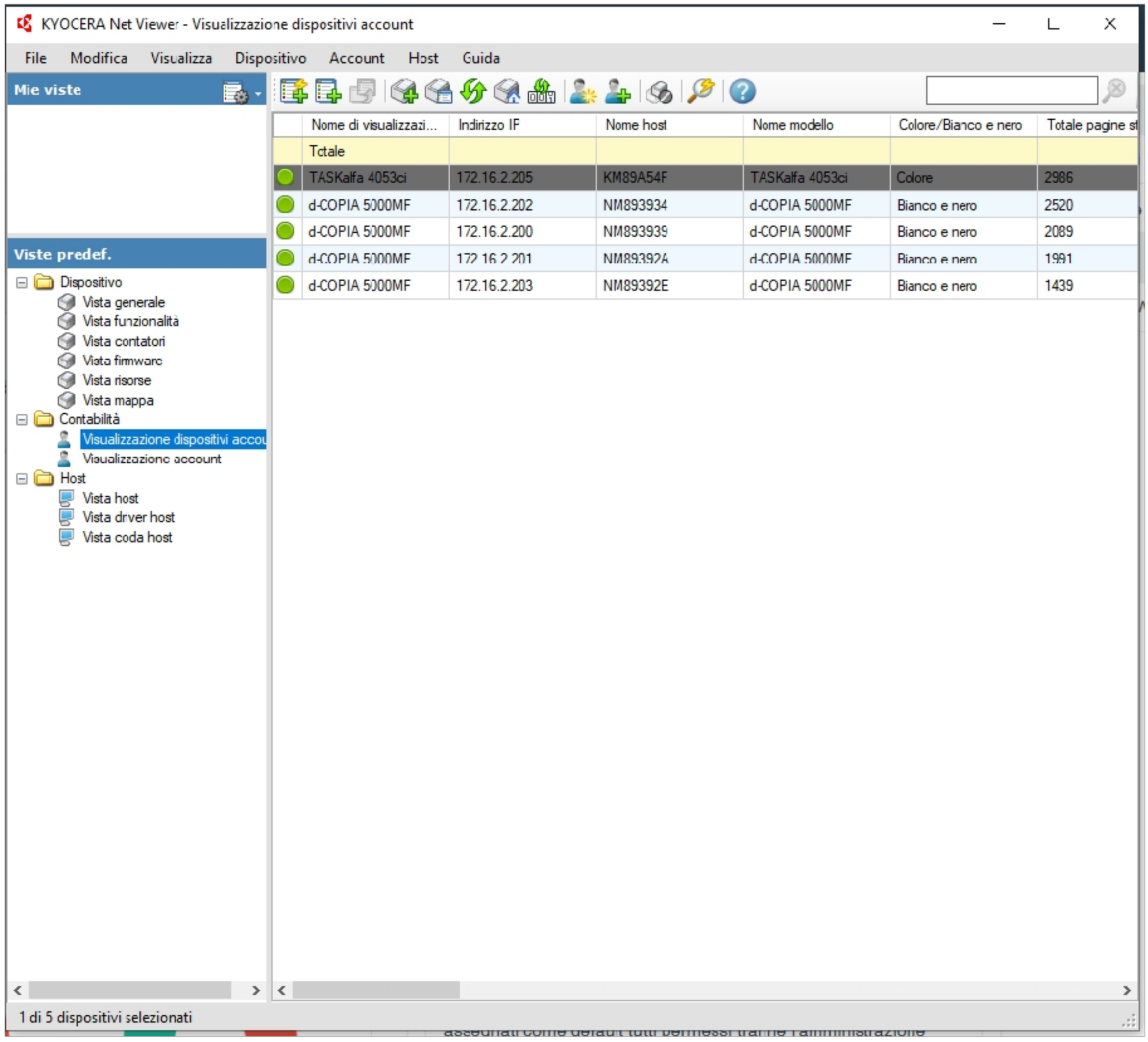
  CAUTION: During installation install all packages, especially accounting.
- In the main menu you will find all the printers in the network, even of different brands.



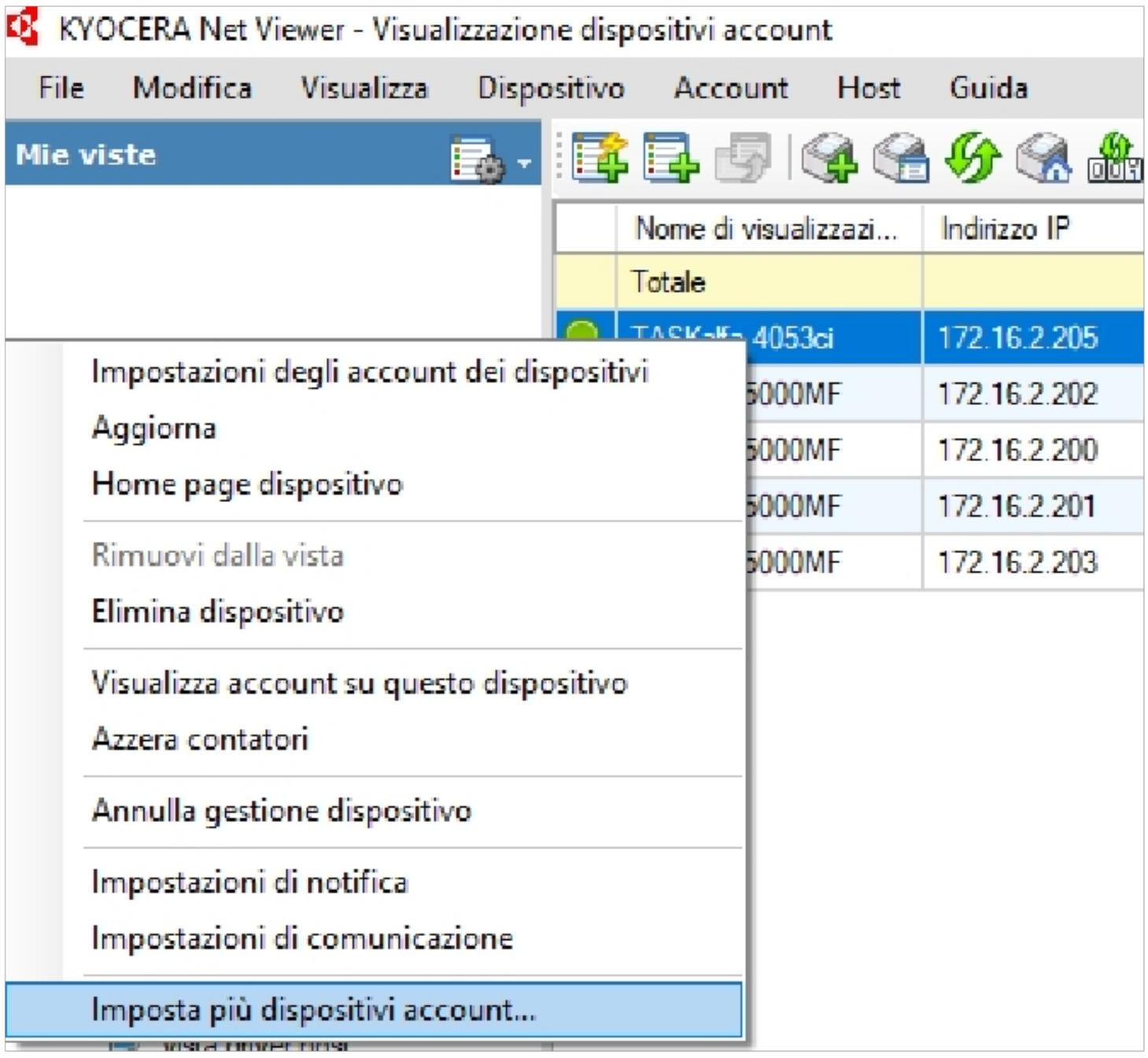
- As shown below, right-click on the desired printer, then on "Communication Settings" and enter username: `Admin` ; password: `Admin`



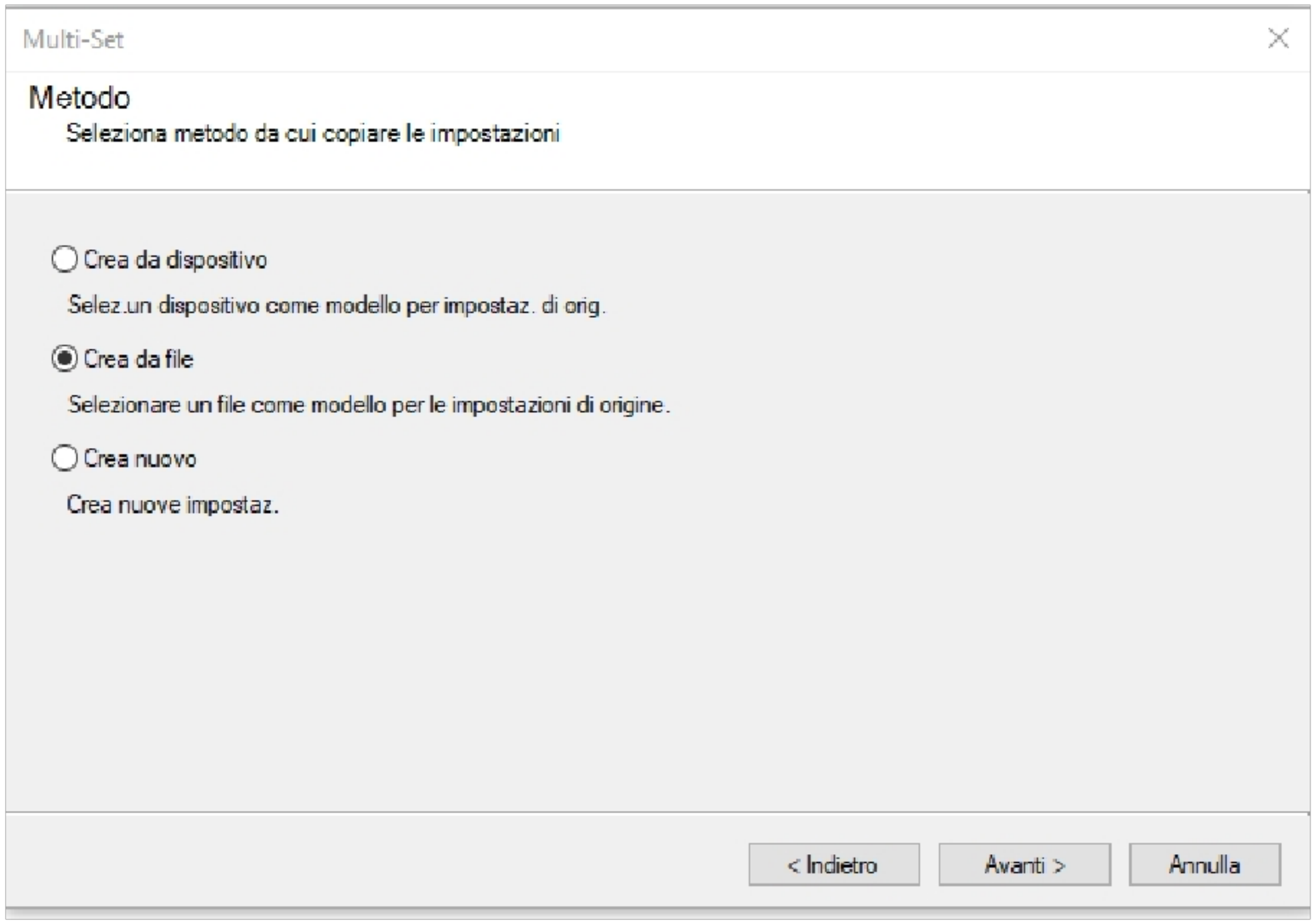
- Account entry (ID, last name and print quota) via fie csv (see the bottom of this tutorial how to create the csv file)
- Place the mouse in the accounting section and activate the desired printer by right-clicking, verifying that the corresponding stamp, from red, turns green.

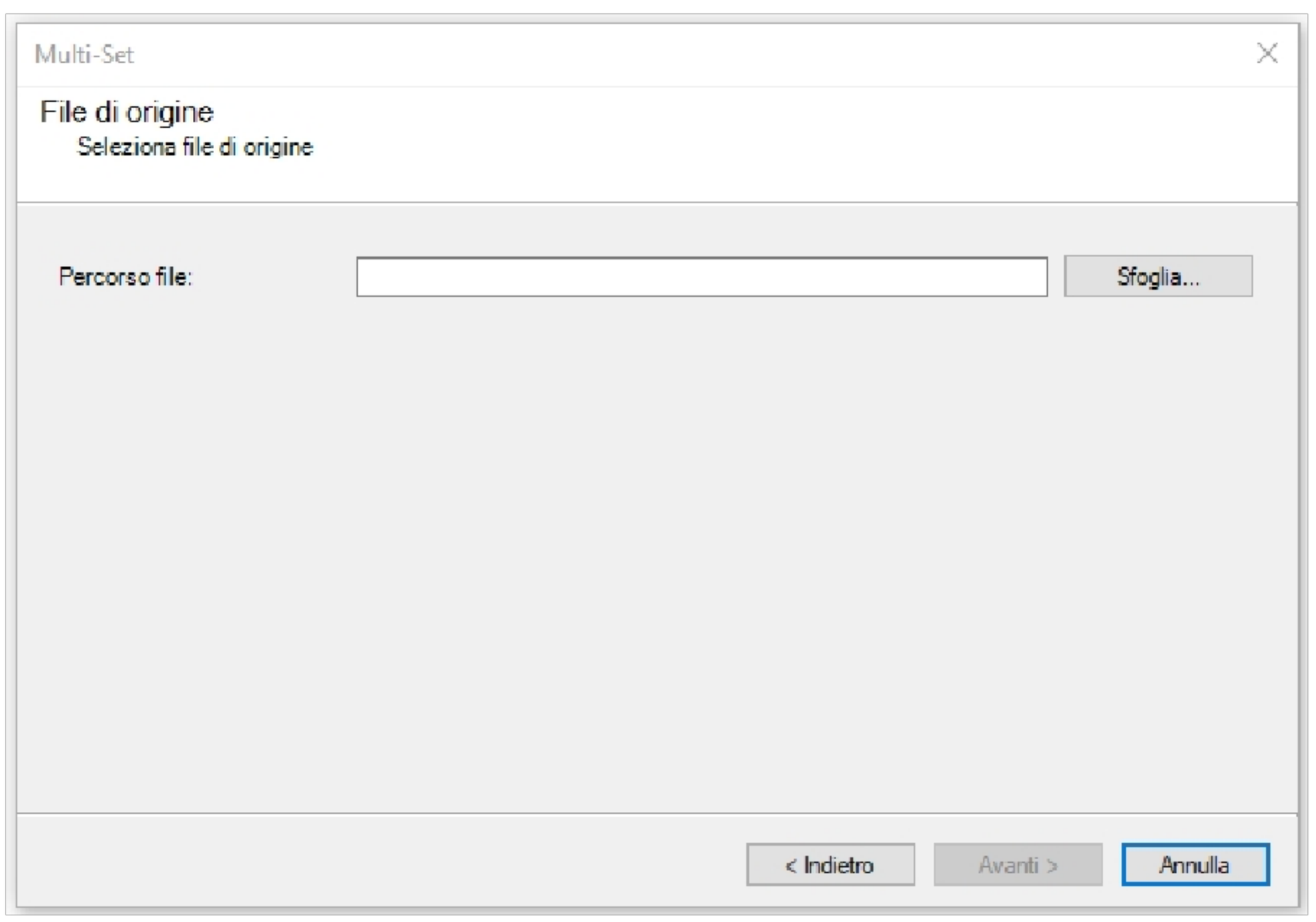


- Right-click on the desired printer and select "Set up multiple account devices."

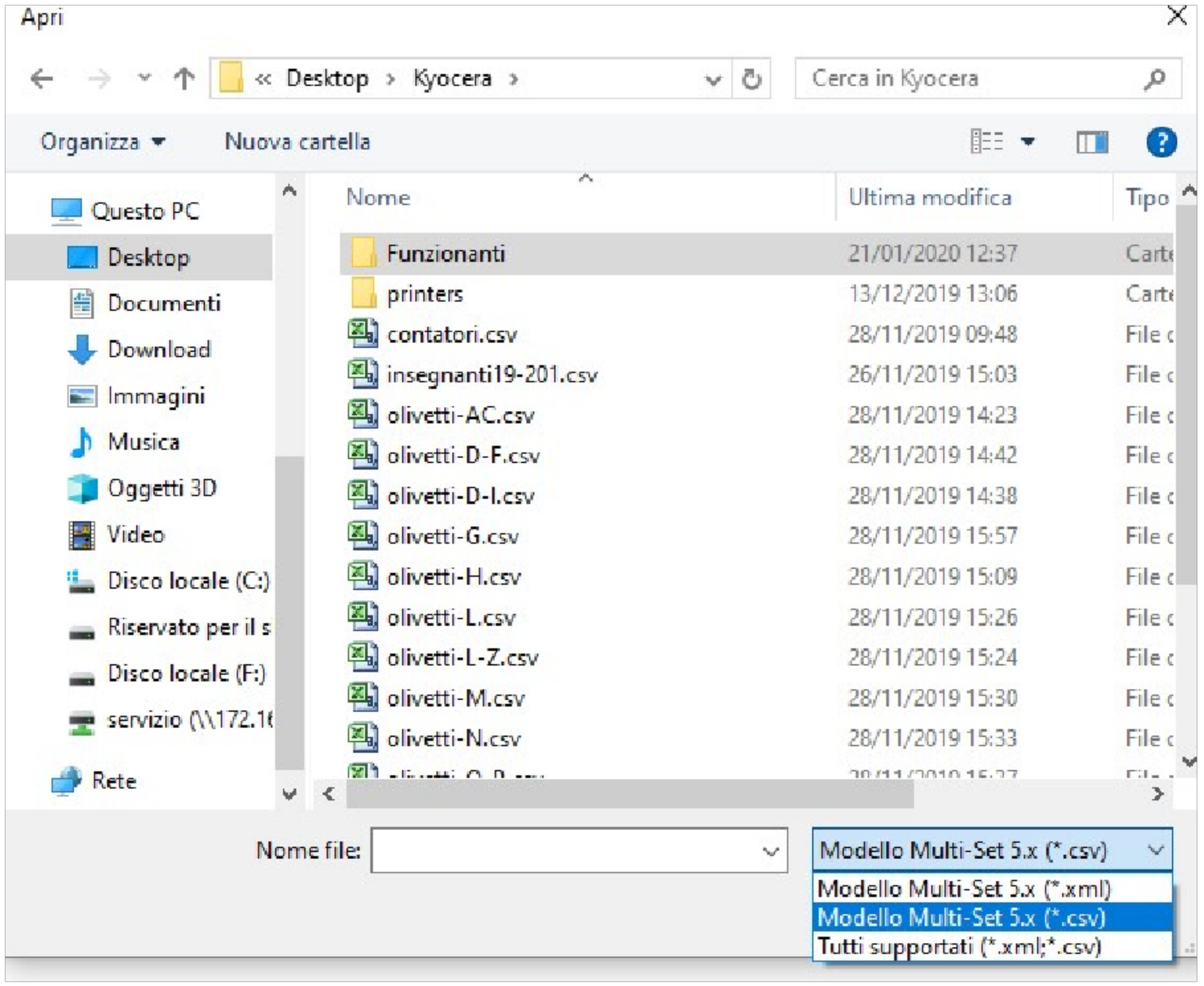


- After choosing the printer model, select `Account Settings`, `Create from File`, and finally click `Browse` to direct the program to the `*.csv` file .





- File selection `*.csv`
- Accounts with the chosen restrictions will be created in the copier



HOW TO CREATE THE CSV FILE

```
| AccountID | AccountName | AccountSubName | PrintTotalR | PrintFullColorR |␣
↪PrintSingleColorR | CopyTotalR | CopyFullColorR | CopySinglecolorR | ScanTotalR ␣
↪| ScanOtherR | FAXTransmissionR | FAXTransmissionPortR |
```

(LibreOffice Calc table template)

- You have to start with a Libreoffice Calc table, corresponding to the template you see above. The table should contain the same 13 fields, with their respective names, entered in the same position. The `*.csv` file must be produced by choosing the DOS format, with the separators , . (semicolon).

12.4 Reader for the health card or CNS/CPS

The current FUSS distribution already incorporates the necessary packages for the operation of the health card reader or CPS/CNS (National/Provincial Service Card) provided by the Autonomous Province of Bolzano. Such packages, by way of information, are:

```
pcscd libccid opensc pcsc-tools
```

To authenticate to Web sites by means of the health card, you must set up (one-time) Firefox to use the OpenSC library according to the following procedure.

1. Open Firefox and go to *Menu -> Preferences -> Privacy and Security*; at the bottom of the page, under the heading *Certificates* click the *Security Devices* button;

2. Click the *Upload* button;
3. Provide in the *Form Name* field a description, such as "National Service Card."
4. To finish set the *Form File Name by* clicking *Browse*, searching and selecting the library `opensc-pkcs11.so` in the following paths:
   - For 64-bit distributions: `/usr/lib/x86_64-linux-gnu/opensc-pkcs11.so`;
   - For 32-bit distributions: `/usr/lib/i386-linux-gnu/opensc-pkcs11.so`.

12.5 Installation of electronic ID card reader

12.5.1 Foreword

The USB NFC reader used in writing this guide is the model `ACR122U USB NFC` Reader from the company Advanced Card Systems Ltd (https://www.acs.com.hk/en/products/3/acr122u-usb-nfc-reader/) and is compatible with major operating systems (Linux, macOS, Windows, Android) with a cost around 40 €.



12.5.2 Installation

- Use a standalone pc with the updated Fuss 10 operating system (buster) that comes directly out of the proxy and make sure that the `pcscd` and `pcsc-tools` packages are installed
- Disable the kernel module `pn533_usb` (which cascades disable "nfc" and "pn533") by creating the file /etc/modprobe.d/cie.conf containing the line:

```
blacklist pn533_usb
```

- download the Home Office middleware by clicking on the following link: https://github.com/italia/ cie-middleware-linux/releases/download/1.4.3.2/CIE-Middleware-1.4.3-3.amd64.deb/ and install it with the command:

```
dpkg -i CIE-Middleware-1.4.3-3.amd64.deb
```

- Configure Firefox, as indicated in the middleware manual:

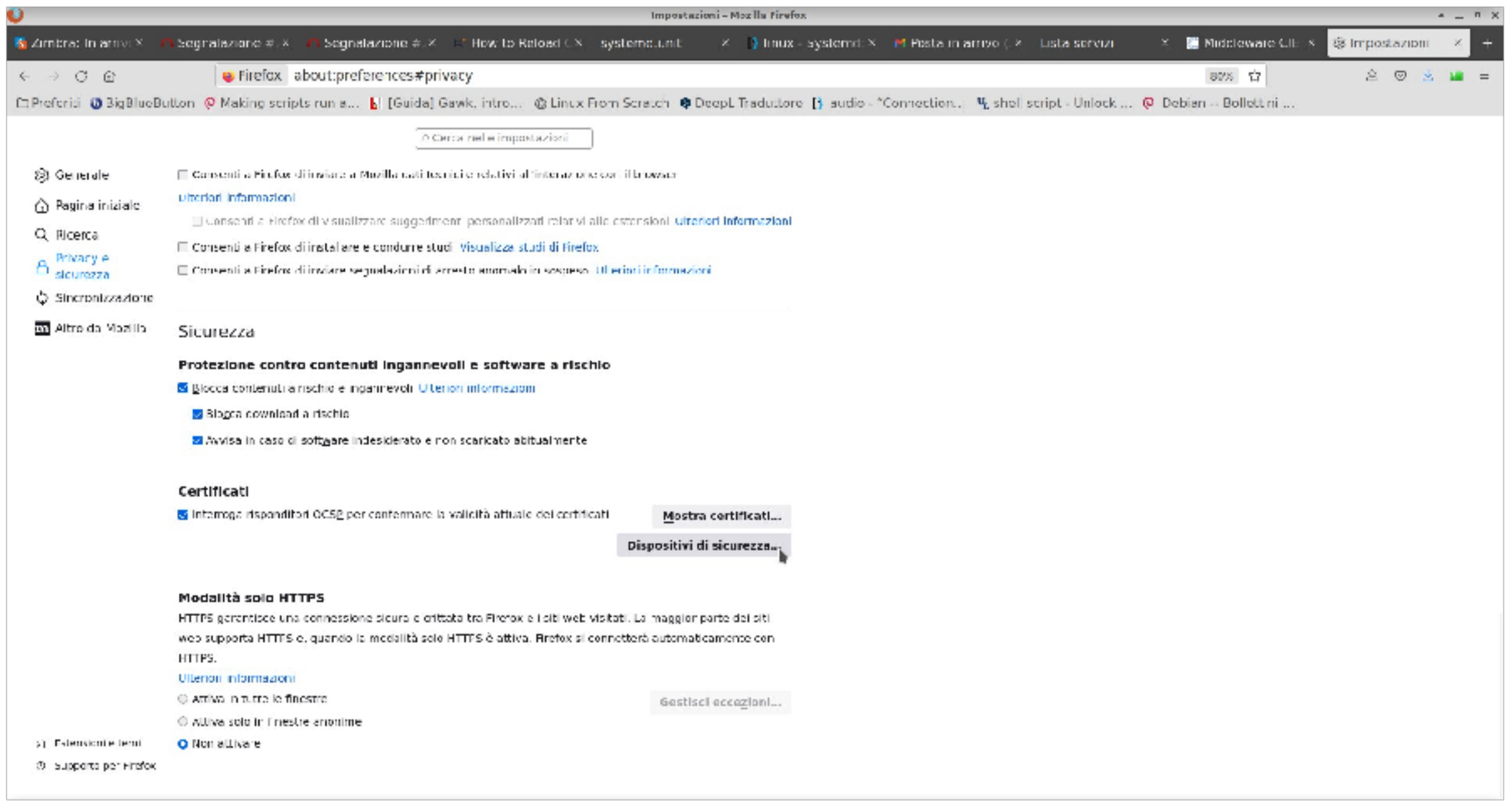
  https://github.com/italia/cie-middleware-linux/releases/download/1.4.3.1/CIE.3.0.-.Manuale.d.uso.del. middleware.Linux.pdf/

  ie:

1. Start Firefox and go to the `Settings` section of the browser:



2. Select the `Privacy and Security` tab



3. Click on `Security Devices`



4. Click on `Upload` and enter the following information:
   - Form Name: **CIE PKI**
   - Module filename: **/usr/local/lib/libcie-pkcs11.so**

Note: In order for the reader to be read correctly, the reader must be plugged in before Firefox starts (otherwise the **pcscd** service is not started).

12.6 Change the disk type of the FUSS Server.

This modification only makes sense if the storage for the disks is LVM-thin; if you are using plain LVM storage, the procedure is useless.

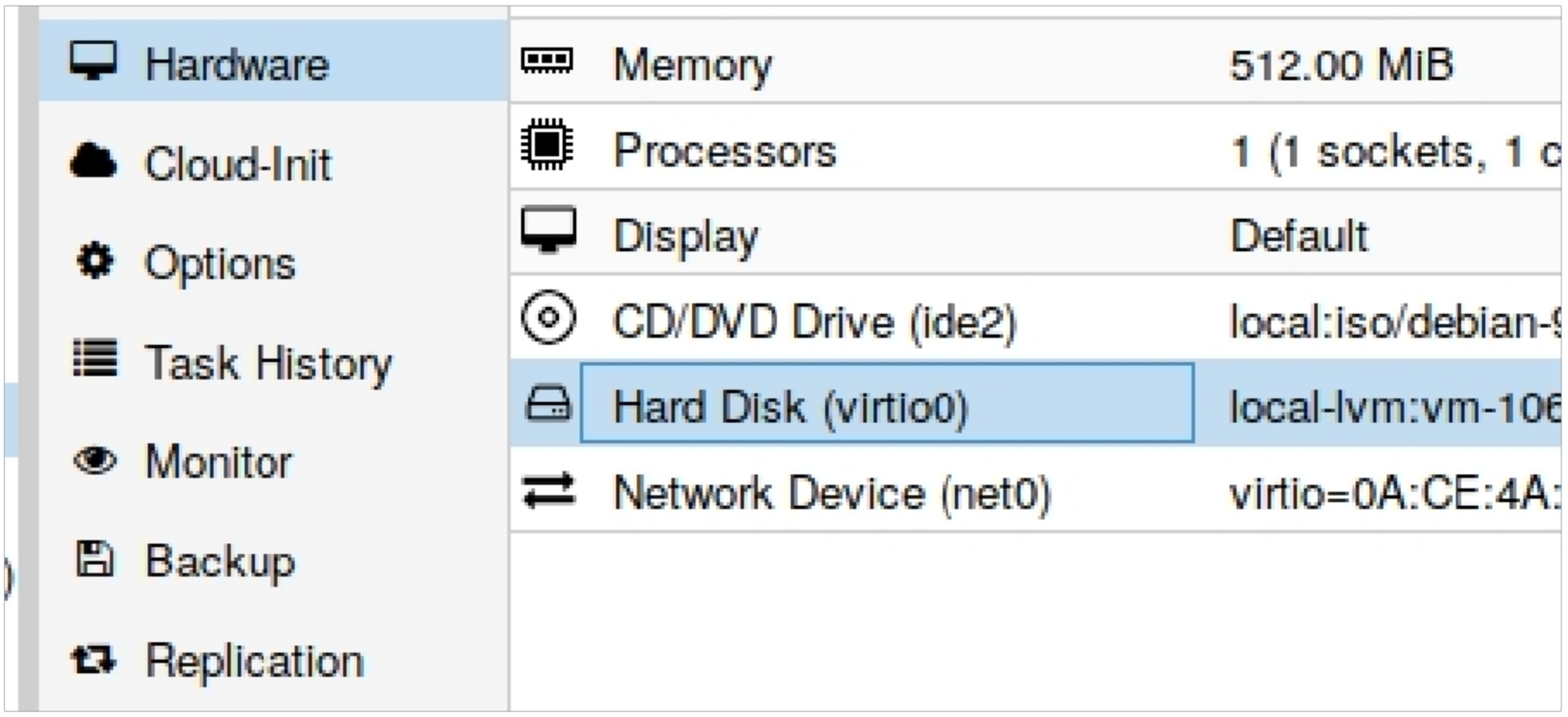
If you have installed the FUSS server or any other virtual machine indicating *VirtIO* or *VirtIO* block (virtual block device) as the disk hardware type, you will not be able to use the `fstrim` command to free disk space occupancy from LVM. This in fact is only realized if the SCSI *discard* command is available, which is supported only by the *VirtIO SCSI* disk type that is the default with Proxmox 5.

To make the change you have to shut down the machine, if its identifier is 100 this is done at the command line with `qm shutdown 100` after which you will have to manually edit the relevant configuration file which is `/etc/pve/qemu-server/100.conf`. The operation has to be done with the machine turned off.

In case you have configured the machine initially with *VirtIO block* the contents of the file will have as configuration for disk identification something like:

```
...
bootdisk: virtio0
...
virtio0: local-lvm:vm-100-disk-0,size=32G
...
```

and will appear in the web interface (by selecting the machine and then the hardware menu) shown as in the figure:



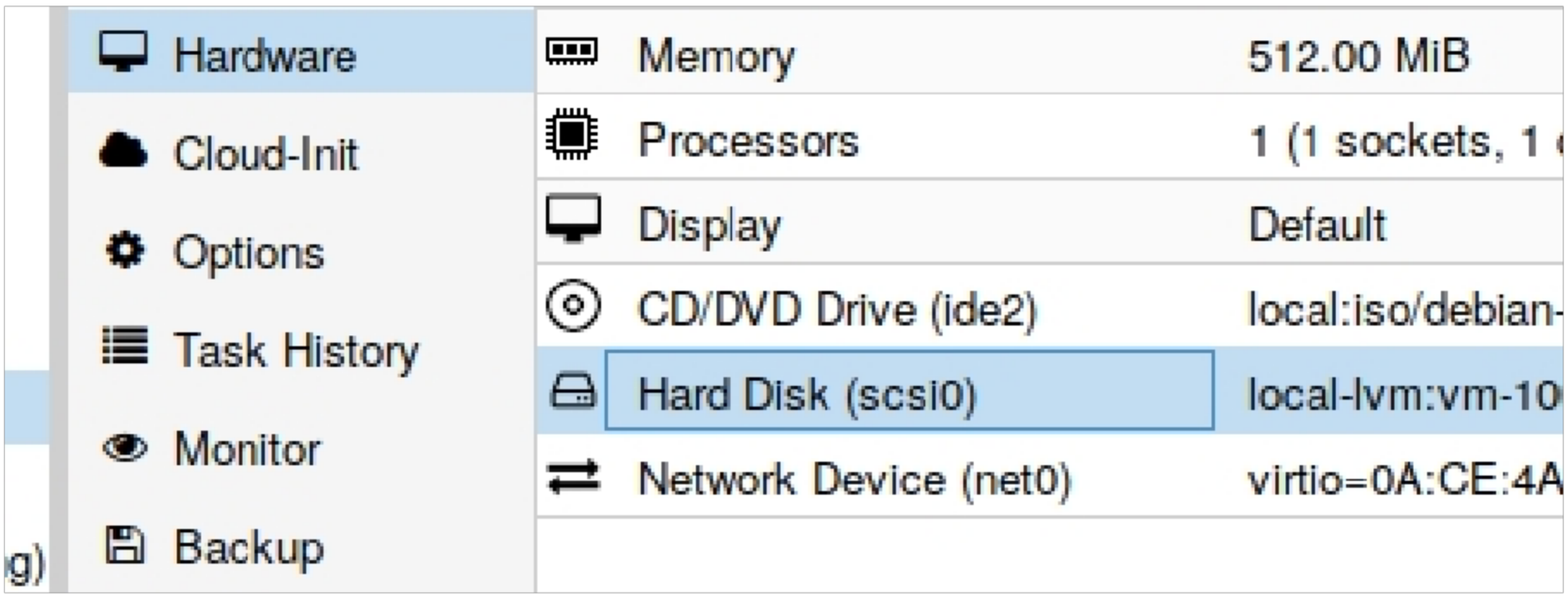
In order to reconfigure the machine to use *VirtIO SCSI* you must first replace `virtio0` with `scsi0` (you are making the assumption of only one virtual disk, if there are more than one the operation will have to be repeated for all of them, indicating with bootdisk which one is to be used as the boot disk); also the type of SCSI media must be indicated with `scsihw` (if not present).

Basically, the configuration file will have to be modified to contain something like:

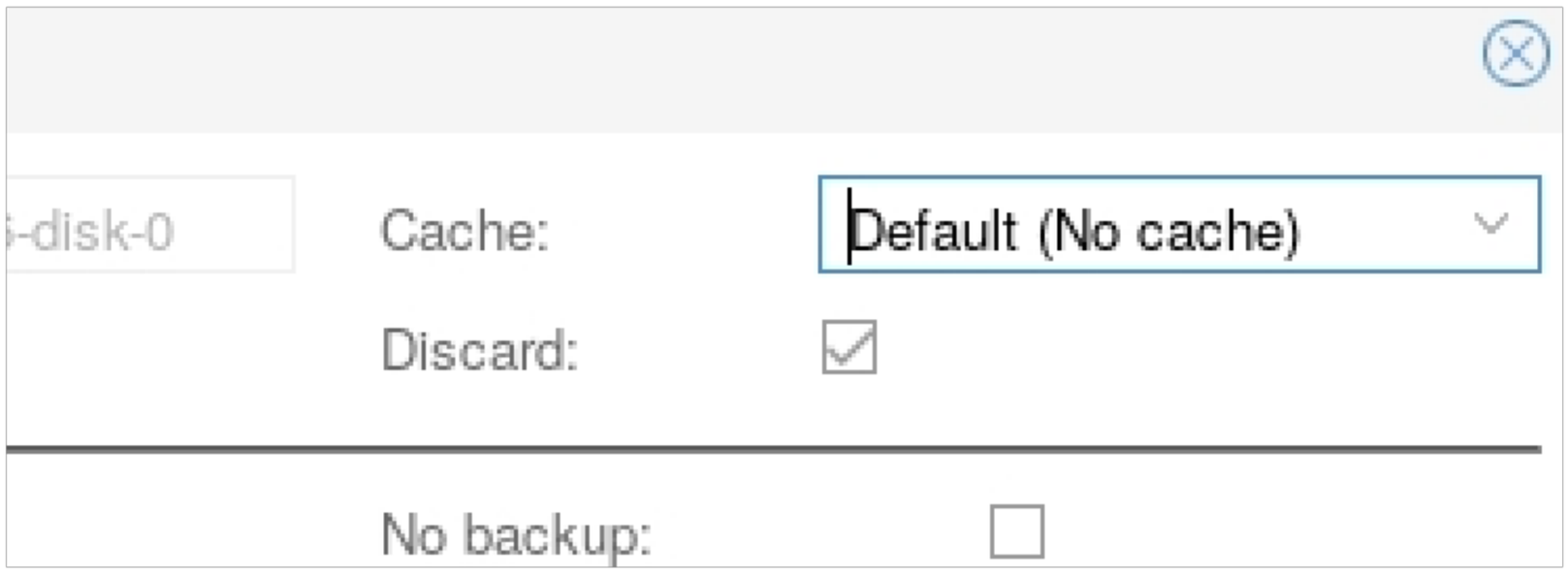
```
...
bootdisk: scsi0
...
scsihw: virtio-scsi-pci
...
scsi0: local-lvm:vm-100-disk-0,size=32G
...
```

As a precaution however keep a copy of the original, this way you can go back at any time by simply copying back the copy and restoring the previous content.

Once the changes are made in the web interface, the disk will be shown in the hardware section of the virtual machine as:



and selecting it will enable the use of the *discard* command, with:



However, this last operation can also be done directly at the editing stage, using it as a disk specification:

```
scsi0: local-lvm:vm-100-disk-0,discard=on,size=32G
```

instead of the previous value. At this point once you restart the server you can use `fstrim`.

12.7 UPS

12.7.1 Foreword

Several such UPSs are currently connected to servers in various schools, without a setup to automatically shut down in the event of a prolonged power failure.

The setup was tested *with USB connection* on *Debian Stretch* operating system (9.4 - ProxMox 5.x).

The UPS models used for the test are as follows:

- **UPS 800 Raptor/Groups**



- **UPS 800 Riello**



- **Braga Moro 1kVA UPS**



12.7.2 Configuration

Installation of the `nut` program (Network UPS Tools)

Launch the command:

```
# apt install nut
```

Configuration of the `/etc/nut/ups.conf` file.

At the end of the file add:

```
[RIELLO]
   driver =
   riello_usb port =
   auto ignorelb
   override.battery.charge.low = 20
   override.battery.runtime.low = -1
```

The name `RIELLO` is as good a choice as any. For Raptors you can put `RAPTOR` or any other name.

Note: The parameter `override.battery.charge.low = 20 is what is` acted on to determine at what state of charge to have the operating system shutdown. If not indicated as in the example the default is 10% (you could increase the value to ensure a safe shutdown).

Note:

- For RAPTOR the driver to put is `usbhid-ups` instead of `riello_usb`
- For BRAGA MORO the driver (compatible) is `blazer_usb`

Having done the configuration we run the command:

```
# upsdrvctl start
```

And we should get something like:

```
Network UPS Tools - UPS driver controller 2.7.2
Network UPS Tools - Device simulation and repeater driver 0.13 (2.7.2)
```

Configuring the file `/etc/nut/upsd.conf`

Here we uncomment the line:

```
LISTEN 127.0.0.1 3493
```

Configuring the file `/etc/nut/nut.conf`

Here we change the `MODE=none` parameter to `MODE=standalone`.

Having done that we run the `upsd` command (to start the daemon). We should then get something like:

```
Network UPS Tools upsd 2.7.2
fopen /var/run/nut/upsd.pid: No such file or directory
listening on 127.0.0.1 port 3493
Connected to UPS [RIELLO]: dummy-ups-RIELLO
```

Note: In case the command gives an error due to the fact that there is already an active instance, just run the command:

```
# upsd -c reload
```

Verification of the state of affairs

With the `upsc` command followed by the name given to the UPS (in the ups.conf file) we can monitor the status of the device. For example:

```
# upsc RIELLO
```

For example, we can see whether the UPS is powered from the mains (`ups.status: OL`) or is taking power from the battery (`ups.status: OB DISCHRG`).

Creating a monitoring user (file `/etc/nut/upsd.users`)

Add to the end of the file:

```
[monuser]
    password =
    mypass actions =
    SET instcmds =
    ALL upsmon
    master
```

Note: This does not involve creating a user on the system, only in the file just seen.

We then do a reload of the configuration with:

```
# upsd -c reload
```

Creating a monitoring directive (`/etc/nut/upsmon.conf`)

Here we find the user we created in the previous file (`upsd.users`). At the end

of the file add:

```
RIELLO MONITOR 1 monuser mypass master
```

With that done, run the `upsmon` command.

At an eventual restart of the machine it should not be necessary to launch the various commands (to be verified . . .with a final test).

12.8 Interactive whiteboards and video projectors

After the configuration of each model is completed, perform a calibration if necessary as indicated in the section of the same name.

Regarding the use of them, as a matter of uniformity in different schools, it is agreed to use OpenBoard software and not proprietary products supplied with the interactive whiteboards themselves.

12.8.1 SMART BOARDS

SMART Board 480

In process

SMART Board M600 (with Epson EB-475W projector)

In process

SMART Board SB680

The following steps are followed for this model:

- Install the xserver-xorg-input-evdev package:

```
apt install xserver-xorg-input-evdev
```

- Rename the /usr/share/X11/xorg.conf.d/10-evdev.conf file by increasing the numeric prefix so that it is greater than 40 (the one in the 40-libinput.conf file):

```
mv /usr/share/X11/xorg.conf.d/10-evdev.conf /usr/share/X11/xorg.conf.d/90-.
↪evdev.conf.
```

If the computer connected to the interactive whiteboard is a notebook, in the file /usr/share/X11/xorg.conf.d/90-evdev.conf comment out the "touchpad" section by letting libinput handle it.

- restart the X server:

```
systemctl restart lightdm
```

If necessary, proceed to calibrate the blackboard as shown below.

SMART Board 800 (with Epson EB-570 projector)

Follow the same steps given for the *SMART Board SB680 interactive whiteboard* .

12.8.2 Hitachi

https://github.com/mmuman/starboard-lsadrv (The makefile is to be reviewed for kernels used by Debian "stretch")

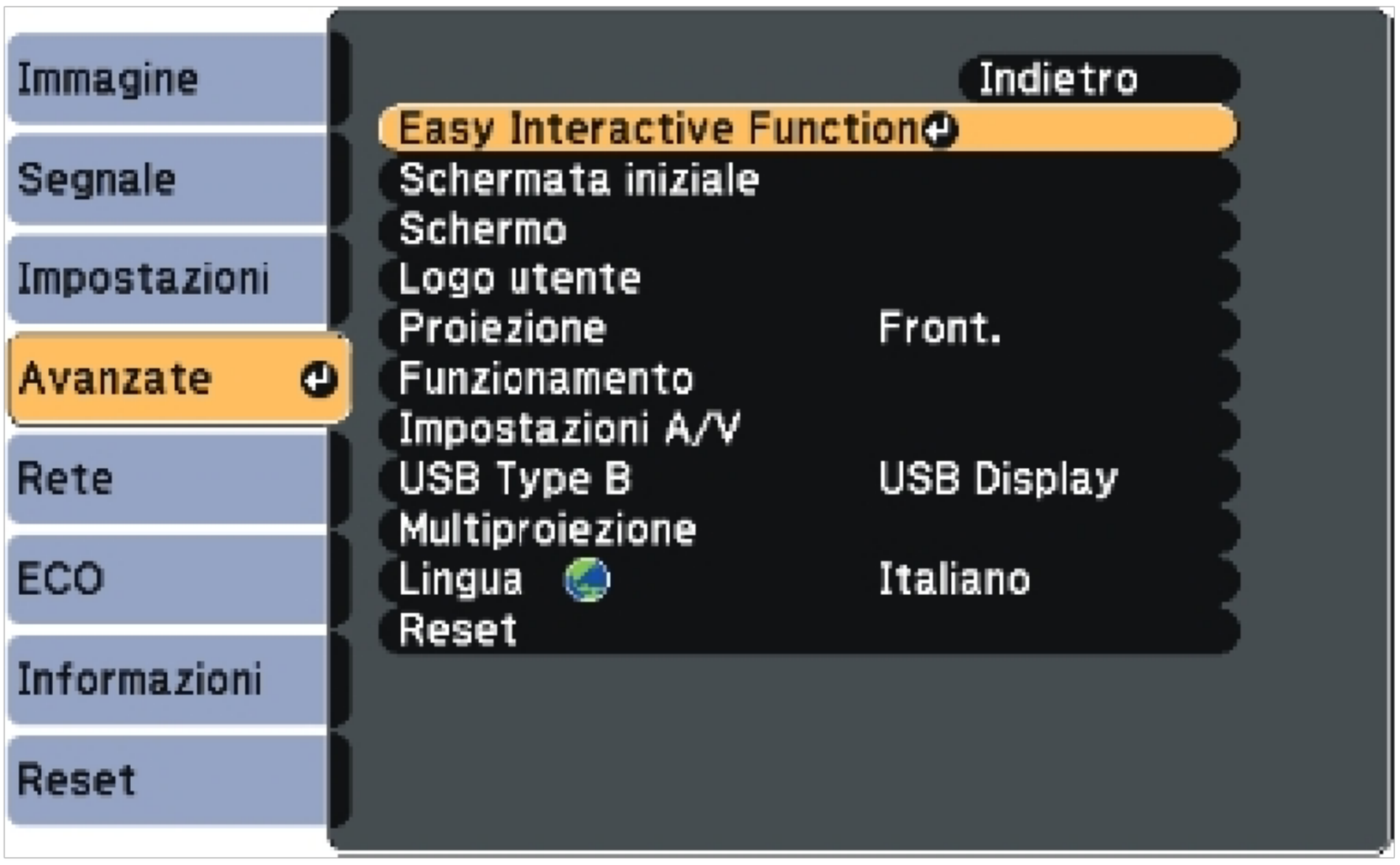
Hitachi Starboard FXT77

In process

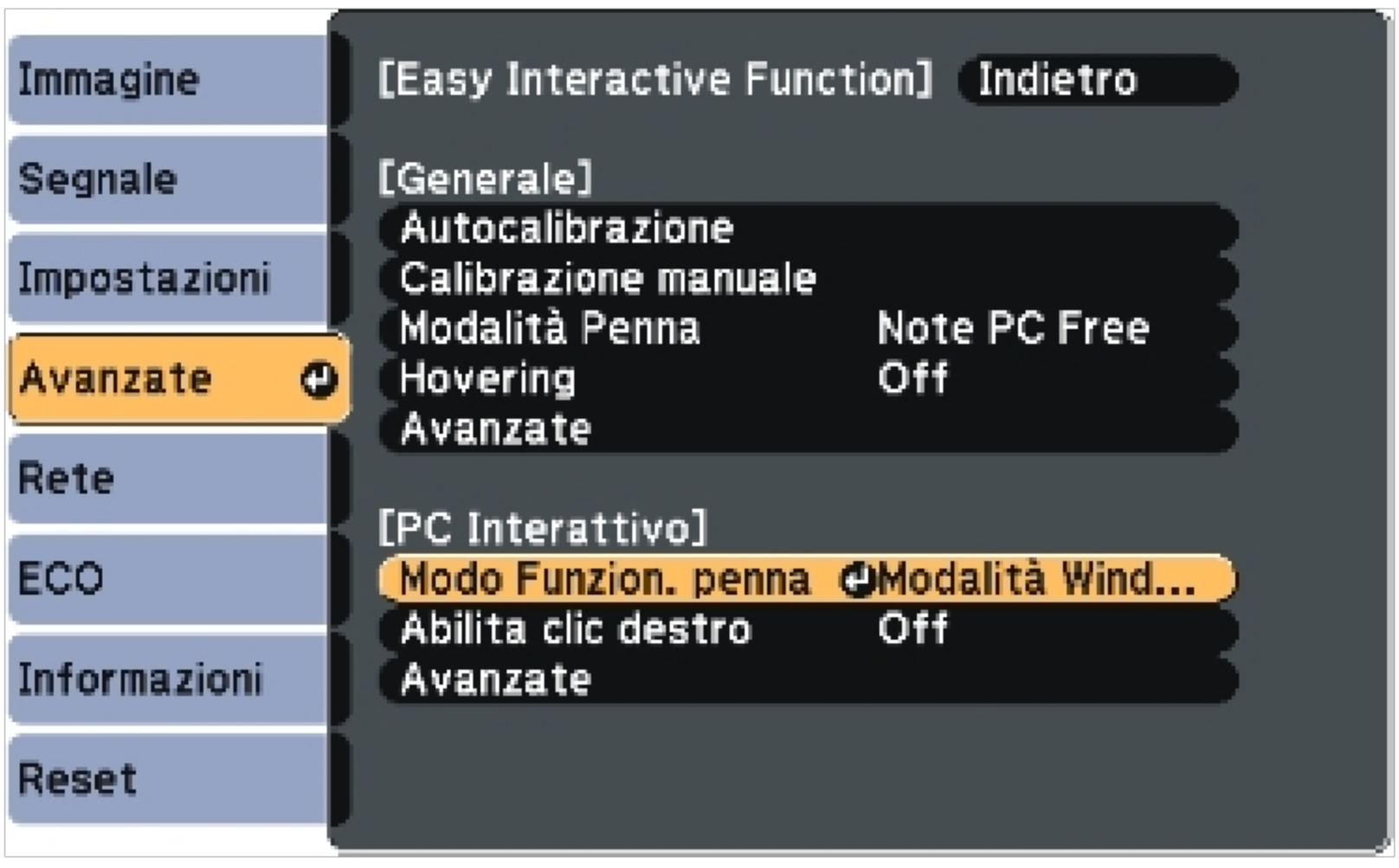
12.8.3 Epson

They do not require additional software for input management. The projector must be properly configured from its Menu. The `Epson EB595 Wi` and `EB695 Wi` interactive projectors allow interactivity through:

- Special supplied pens (pens) based on infrared technology
- Finger touch (finger touch) based on laser technology

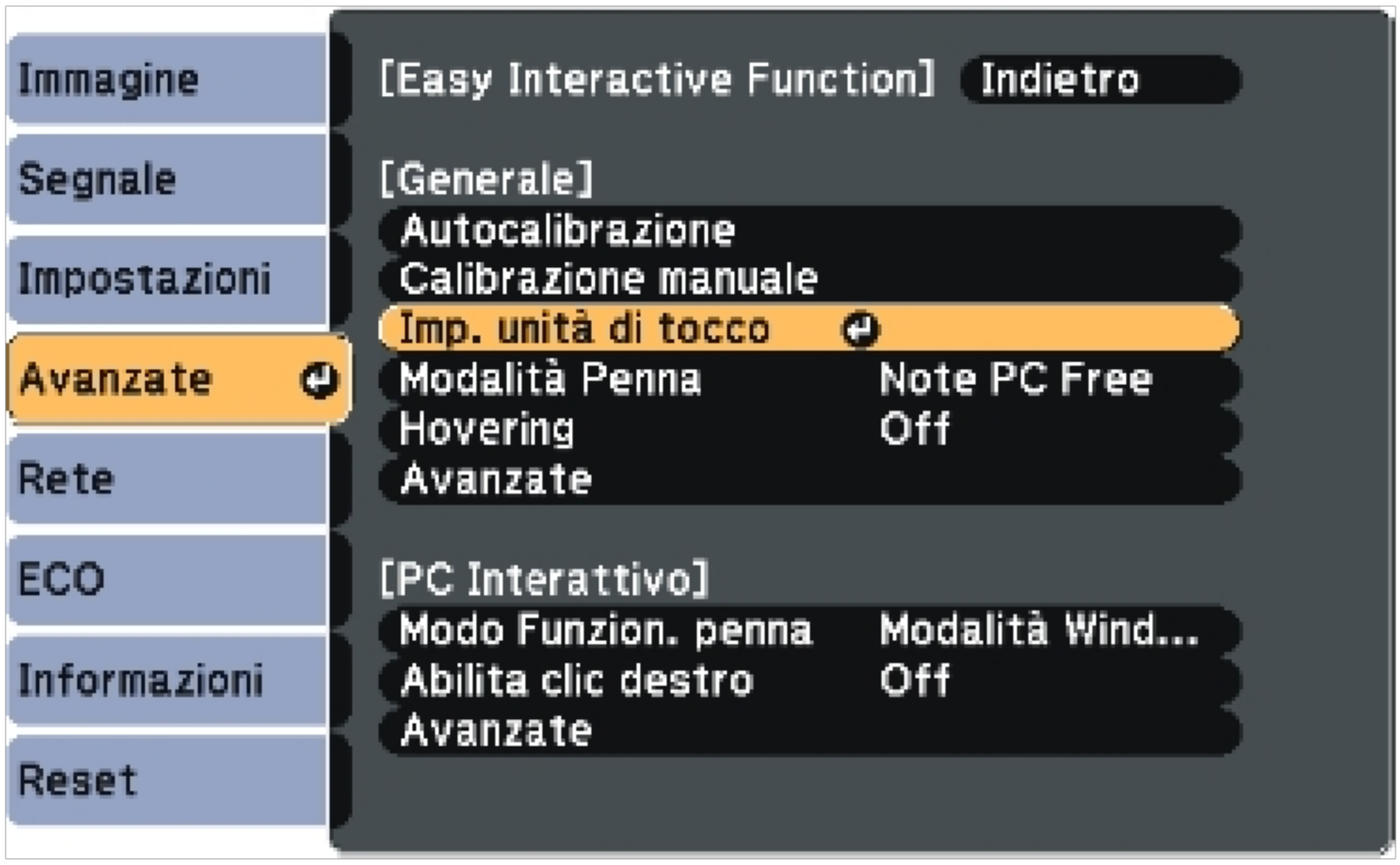


To activate the `interactive pen` feature, one must select:

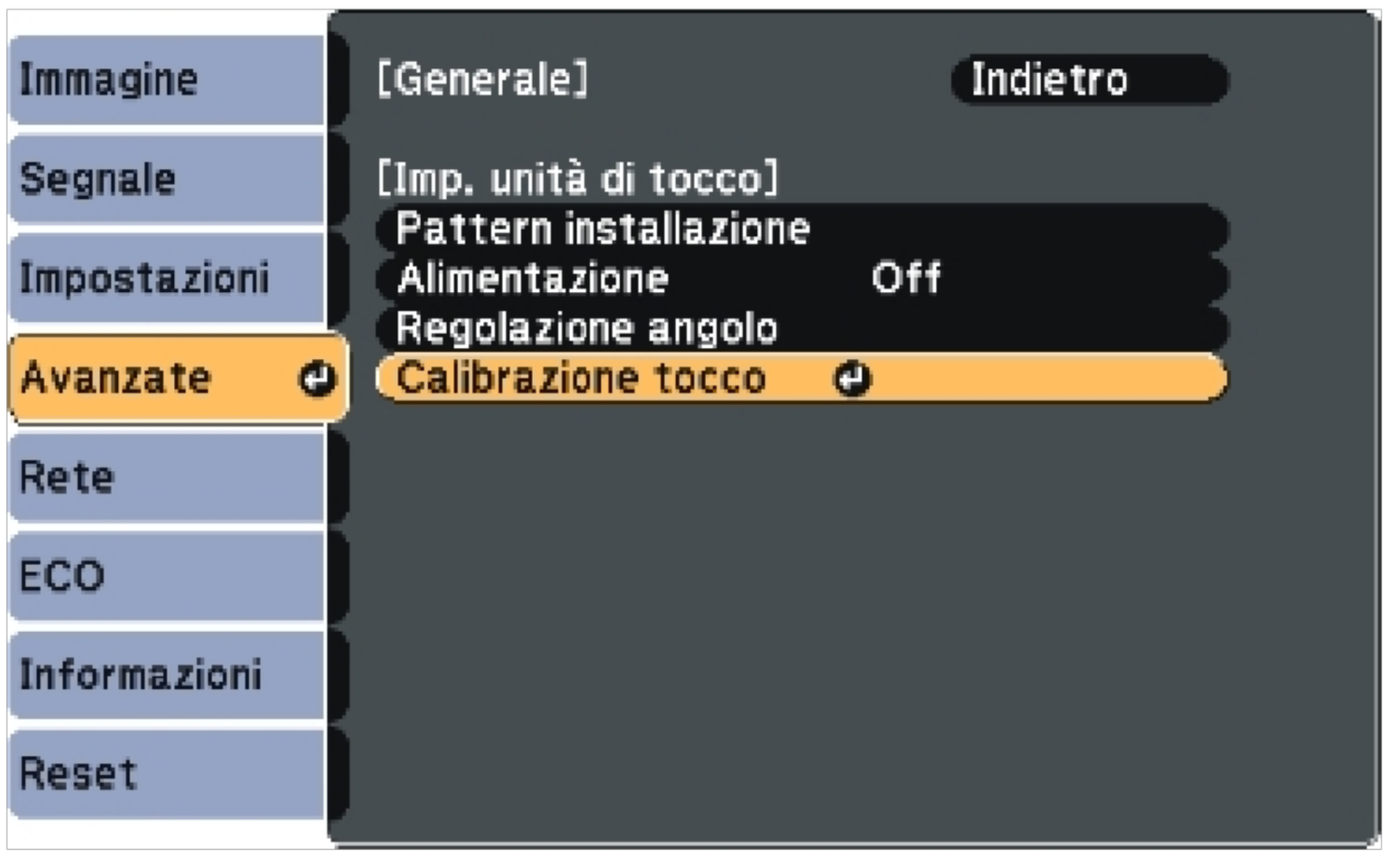


- Select the setting `Operation Mode. Pen` and press the [Enter] key.
- Select `Ubuntu Mode` and exit.

To activate the `finger touch` feature, one must select:



- Select `Set Touch Unit` and press the [Enter] key.
- Select `Power` and press the [Enter] key.
- Select On and exit.



Perform a calibration if necessary. Refer to the manual for this and other configurations that may be needed:

> https://www.ceconet.ch/data/dokumente/00002981/Italienisch/Support/Anleitung/Instruzioni%20per%20l'uso_EB-695Wi-685Wi-680Wi-675Wi-685W-675W-680-670_IT.pdf

12.8.4 Samsung Monitors

Samsung DM65E-BR requires no additional software to operate the touchscreen.

12.8.5 QOMO QWB100WS-PS

For this model, follow the same steps given for the *SMART Board SB680 interactive whiteboard* . If necessary, proceed to calibrate the board as shown below.

NOTE: DO NOT use the old drivers that were downloadable from:

- https://drive.google.com/file/d/0B_NIgwPdq93QRC1BdGt2QTNILUU/view?usp=sharing

or from

- https://nc.fuss.bz.it/index.php/s/WWYoX5rHMtMLrNK

12.8.6 Calibration

If not present, install the `xinput-calibrator` package Run the application as root:

```
xinput_calibrator --list
```

and note down the ID (numeric) of your input device (whiteboard). Important to locate the device correctly since there may be other input devices (e.g., notebook touchpad). Then run the xinput_calibrator command again with the following parameters:

```
xinput_calibrator --output-filename /usr/share/X11/xorg.conf.d/99-calibration.conf ␣
↪--device ID-The-Slate.
```

and proceed to calibration. When the calibration is completed, the above file will be written which will contain a configuration similar to the following:

```
Section "InputClass" Identifier
                  "calibration"
    MatchProduct    "EPSON EPSON 695Wi/695WT"
    Option    "Calibration"    "55 32624 -10 32331"
    Option    "SwapAxes"    "0"
EndSection
```

In case of misclick detection during calibration, reduce the projection area on the board and relaunch the calibration command. Finally, restart the X server:

```
systemctl restart lightdm
```

12.8.7 Optimal mirroring of two video devices connected to the same pc

---

Note: Since the Fuss 10 distribution, the configuration of the Xserver graphics server no longer relies on the xorg.conf file that used to be placed in the /etc/X11/ folder.

The latest `fuss-client` installs on all machines the `autorandr` package and an `arandr-setup` script That was put in `/usr/sbin`.

In many cases autorandr can automatically find the optimal mirroring. In case it fails to do so or you want to obtain a custom pair of resolutions you should proceed as follows.

Only on machines connected to projectors/LIMs/monitors for which a solution is desired, or needed "customized."

1) you log in as root
2) you launch the `arandr-setup` script
3) you choose the best "mirrored" resolution on both screens

The contents of the `arandr-setup` script are as follows:

```
#!/bin/bash
arandr
autorandr --save $HOSTNAME
mkdir -p /etc/xdg/autorandr/
cp -r /root/.config/autorandr/$HOSTNAME /etc/xdg/autorandr/
```

The script allows you to create a "custom" video configuration, shared by all users. If necessary, it can later be modified by re-launching the same script.

Restart the PC and verify that the resolution is the one chosen:

- either before login
- either after logging in

To avoid interference from any configurations made via `xfce4-display-settings` and saved in `~/.config/xfce4/xfconf/xfce-perchannel-xml/displays.xml`, server-side a cron-job `/etc/cron.d/home-cleanup` was provided for periodic deletion of `displays.xml` to users.

CHAPTER 13

Software miniguides

This section includes guides on various topics of utility in schools related to installations for particular hardware.

13.1 Configuring fuss-server to enable mail sending

Direct sending of e-mail messages from machines on the internal network (LAN) of the Fuss Server is disabled for security reasons. If for specific needs (such as using the "scan to mail" feature of multifunction printers), it is necessary to allow a machine or apparatus to send mail, the following instructions can be used in order to rely on the Fuss Server for sending.

The Fuss Server does indeed have the Postfix SMTP server installed, but it is configured to accept mail to be sent only from `localhost`. The `mynetworks` directive, which controls which machines can send mail through the server, is found in the file `/etc/postfix/main.cf` and its default value is as follows:

```
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
```

In order to allow other machines or equipment such as a multifunction printer to send mail, you must first have the IP address; you must also take care to set it statically so that it does not change when the printer is restarted.

Once the IP address is known, you will need to add it to the list of the one allowed by `mynetworks`. The directive, as the name implies requires a list of networks so if only one IP is given you will need to use CIDR notation by adding the suffix `/32`. The list of networks must be provided as a space-separated list, you can wrap and write it over multiple lines, taking care to start each extension line with spaces.

For example, if you have multifunction printers that use "scan to mail" with IP addresses `192.168. 0.10`, `192.168.0.15`, and `192.168.0.20` to allow them to send mail outward via the Fuss Server you will need to change the previous configuration to:

```
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
   192.168.0.10/32 192.168.0.15/32 192.168.0.20/32
```

and restart the service with `service postfix restart`.

At this point you can configure the printer (or other equipment) by indicating the fuss server itself as the SMTP server.

Note: It is recommended for safety to use the server's IP address, which will continue to work even if the printer cannot resolve the names assigned to machines on the internal network.

13.2 Problems with CDs and DVDs

13.2.1 Assembly of CD-ROMs

Problem in mounting

CD-ROMs are automatically mounted in `/media/cdrom0`. This is due to the fact that in `/etc/fstab` the following line is found:

```
/dev/sr0        /media/cdrom0udf,iso9660 user,noauto          0       0
```

For some instructional DVDs, such as Zanichelli DVDs, this is a serious problem, because the script that is launched rigidly requires that the DVD be mounted in `/media/<user-name>`.

In addition, the contents of the CD do not have the user as the owner, and all files and directories are assigned to `nobody:nogroup` (i.e., they are not assigned).

Solution of the problem

In order to do this, you have to make sure that the above line is not read in `/etc/fstab`. The

following script solves the problem:

```
#! /bin/sh
if [ ! -f /etc/fstab-old ]
then
    cp /etc/fstab /etc/fstab-old
fi
sed -i 's/^\/dev\/sr0/#/\/dev\/sr0/' /etc/fstab
```

Restarted the PC the DVD-ROM is mounted in `/media/<user-name>/<cd-name>`

13.2.2 Zanichelli DVD

Zanichelli's DVDs in the "Ideas for Teaching with Digital" series can be viewed with our distribution, as long as we first install certain packages, on which program execution depends.

The following script allows installation of the packages you need:

```
#! /bin/sh
echo "deb http://ftp.de.debian.org/debian/ jessie main" >>/etc/apt/sources.list
apt update && apt upgrade
apt install libpng12-0 gstreamer0.10-fluendo-mp3 gstreamer1.0-alsa gstreamer0.10-
↪alsa
```

Open a terminal and as the user, type the following command:

```
sh /media/<user-name>/<cd-name>/BooktabZ-StartCD_lnx.sh
```

13.2.3 Installation of Oxford DVD-ROMs on FUSS 9

Foreword

The following procedure applies only to 64-bit machines since the software is not compatible with 32-bit Debian 9.

"It was developed for DVD-ROMs in the `New Treetops` series but also applies to other Oxford products such as `High Five` .

Problem in mounting

DVD-ROMs are automatically mounted in `/media/cdrom0` and by default are not executable. This is because the following line is found in `/etc/fstab`:

```
/dev/sr0        /media/cdrom0udf,iso9660 user,noauto         0       0
```

Solution of the problem

You have to make sure that the DVD-ROM is reassembled in executable mode. Insert the cdrom and from terminal launch as root:

```
mount -o remount,exec,ro /media/cdrom0
```

Installation

To install, enter `/media/cdrom0` and run the `setup-linux-x64` executable, which opens the installation wizard. When the installation is finished, click `Finish` in the wizard and `Ok` in the README window. At this point you can unmount the DVD-ROM.

Starting the program

A `~/Oxford University Press/` folder is created in the installer's home, which contains a subfolder for each DVD-ROM in the series.

For example, to start the second volume you follow the path:

```
~/Oxford University Press/New Treetops 2a/linux-x64/ # Obviously enter the␣
↪backslash if working from terminal.
```

and you launch the `oup` executable (in volume 3 you launch `New Treetops 3a`).

Installation adobe-flashplugin

Viewing the application videos requires adobe-flashplugin. Fortunately, a hidden subdirectory is created during installation (~/Oxford University Press/New Treetops 3a/.flash_installers/linux-x64/) that contains some debian packages of adobe-flashplugin. If it is present, remove flashplayer-mozilla:

```
apt remove flashplayer-mozilla
```

Install one of the adobe-flashplugin packages (the following command file was tested):

```
dpkg -i adobe-flashplugin_11.2.202.280-0precise1_amd64.deb
```

Shared folder

The folder containing the installations from the DVD-ROMs can be copied to a folder shared by the teachers and possibly the pupils. The owner of the folder is preferable to be root to avoid unintentional deletions, while the owner group should only have read and execute permissions. Alternatively, read and execute permissions are left to all.

Possible desk launcher

If you prefer to launch applications from the desktop, you can create launchers:

```
1) Right-click

2) Select ``Create starter``

3) Choose a name and command with care to insert backslashes before
↪blank spaces.
   For example, the command to launch New Treetops 2a will be::

   ~/Oxford\ University\ Press/New\ Treetops\ 2a/linux-x64/oup

substituting the tilde ~ for the full path to the user's home or the
↪sharedfolder.
```

13.3 Chromium settings

13.3.1 Foreword

The following mini-guide arose from the need to solve two problems:

1. When the chromium browser is started, it is insistently asked to enter the keychain unlock password
2. Several users would like proxy login credentials to be stored without having to be typed in each time.

13.3.2 Solution to problem 1

a. From root

   Modify the chromium launcher:

```
vim /usr/share/applications/chromium.desktop
```

   Change within the file the command to be:

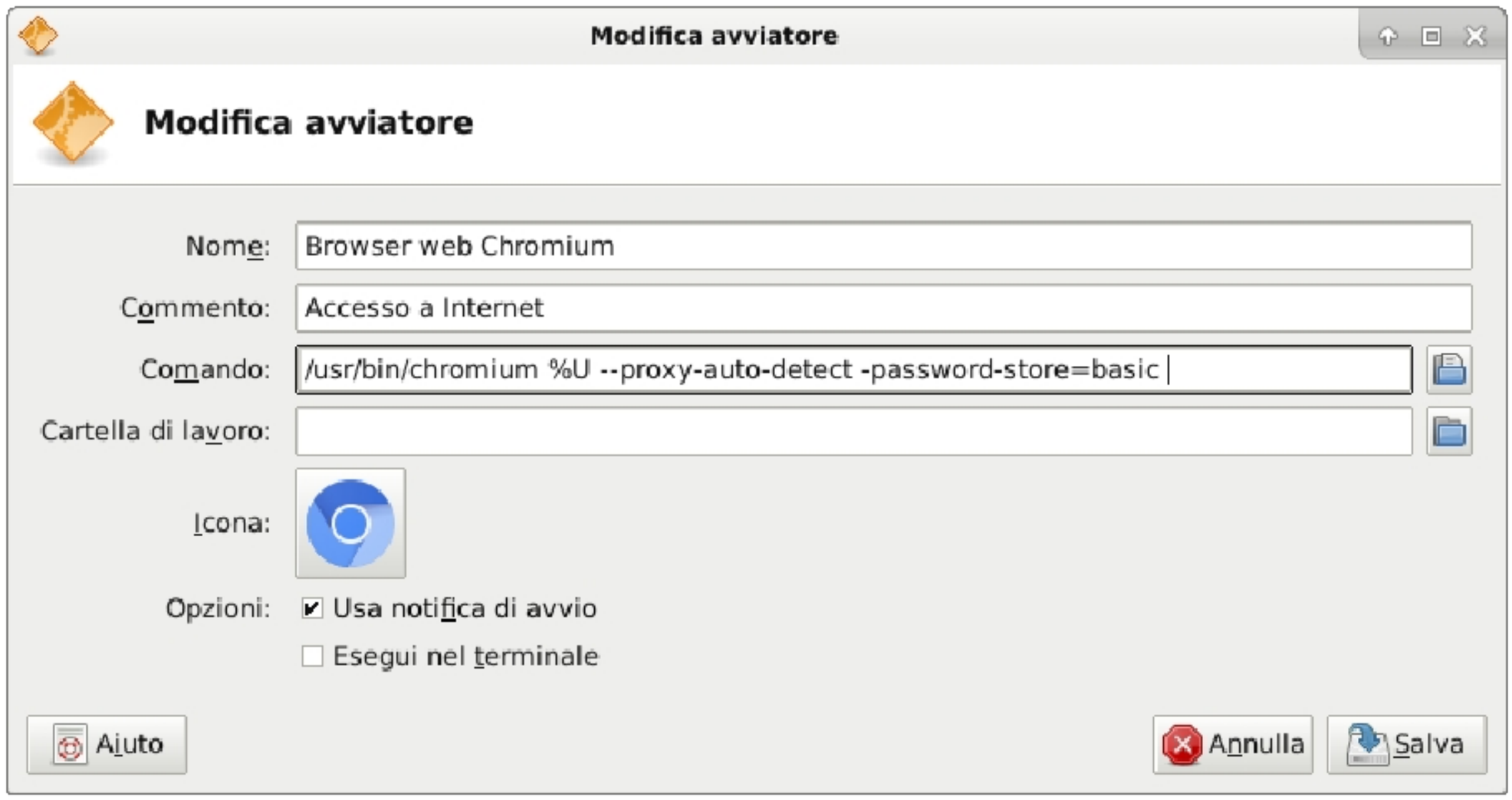
```
Exec=/usr/bin/chromium -password-store=basic %U
```

b. As a normal user

- Create a launcher by dragging the chromium browser icon from the menu to the panel and confirming.
- Right-click on the launcher and select `Properties`. The window opens:



- Click on `Edit the selected item`
- Add to the Command line the string `-password-store=basic` (possibly also `--incognito` if you want to browse "anonymously").



13.3.3 Solution to problem 2

- The offer to save proxy credentials occurs unpredictably and is difficult to replicate; sometimes it occurs by deleting the ./config/chromium folder and unchecking `Automatic Login` in Settings > People > Passwords.
- The easiest and most certain way to achieve this is to use a downloadable extension from the `Web store` that stores proxy credentials, which will not be requested again.

  Of course, the user must remember to update them when the account password is changed.

13.4 Installation of the iprase game package

13.4.1 Foreword

It is a collection of educational games for compulsory school children. IPRASE, adhering to the experimental project within the framework of European Social Fund co-financed activities on Teaching Assisted by New Technologies, carried out an experiment in compulsory school for three consecutive years starting from the 2001-2002 school year. The objective of the initiative was to provide useful tools for the introduction of new technologies into the teaching and daily work practice of teachers. The experimentation was aimed at elementary and middle school teachers and pupils. It proposed the use of games and exercises to be done on the computer and concerning knowledge and skills in the following disciplines: Italian, Geography, Mathematics.

Although several years have passed, the games are still popular. Their use and packaging has been allowed.

13.4.2 Addition of i386 architecture

To run, the application (based on .exe executables), requires the use of wine and the i386 architecture, which can be added with the command:

```
dpkg --add-architecture i386
```

To update the cache with i386 packages you launch:

```
apt update
```

Finally you install the application with:

```
apt install iprase
```

13.4.3 Local installation with .deb package

In case you have downloaded the iprase_1.1.deb package locally, add the i386 architecture and after apt update and apt dist-upgrade simply launch:

```
dpkg -i iprase_1.1.deb
```

13.5 Share Samba with subfolder structure

The Samba share structure supported by OctoNet allows only a flat list of shares.

In special cases, a hierarchical structure may be necessary, such as the following, where there are two folders, `teachers` and `pupils`, and:

- The faculty folder can only be accessed by those who belong to the faculty group;
- the pupil folder has within it the class folders that they can access:
  - pupils belonging to the class group, to their class file only;
  - teachers, to the folders of the classes to whose group they belong (as a secondary group assignment from OctoNet).

In this case it is necessary to create folders with the following permissions on the filesystem:

```
root@serverlnx:~# ls -l /home/SAMBA/public/ -a
total 16
drwxrwsr-x 4 root teachers 4096 Mar 12 15:41 .
drwxr-xr-x 9 root root       4096 Mar 12 15:41 ...
drwxrwsr-x 5 root teachers 4096 Mar 12 15:41 pupils
drwxrws--- 2 root teachers 4096 Mar 12 15:41 faculty
```

(`2775` for directories also to be accessed by alumni (`/home/SAMBA/public/` and `/home/SAMBA/public/alumni`) and `2770` for faculty where they do not have to reach); e:

```
root@serverlnx:~# ls -l /home/SAMBA/public/alumni/
total 12
drwxrws--- 2 root 1a 4096 Mar 12 15:41 1A
drwxrws--- 2 root 1b 4096 Mar 12 15:41 1B
drwxrws--- 2 root 1c 4096 Mar 12 15:41 1C
```

(permits `2770` and group assigned to the class).

The samba configuration, to be added in `shares.conf` will then be:

```
[public]
path = /home/SAMBA/public
guestok = no
readonly = no
create mask = 0660
directory mask = 2770
readlist = @Domain+Users
writelist = @teachers
```

13.6 Updating fuss-clients via fuss-cru

To upgrade fuss-clients from one fuss version to the next, the `fuss-cru` package can be used. The versions 11.* of that package support upgrading from fuss 10 (buster) to fuss 11 (bullseye).

Warning: Mass upgrade of a classroom from fuss 11 to fuss 12 (bookworm) is not supported, for which reinstallation via fuss-fucc / clonezilla is recommended instead.

- First, make sure you have upgraded `fuss-server` to at least version 10.0.45, and launched `fuss-server upgrade`: this is necessary to enable debian package caching and make the upgrade faster.
- Install the `fuss-cru` package on the fuss-server; this will automatically create a new script in octonet.
- add a run of the clientupgrade script on octonet and schedule it as usual.

Note: Remember that `octonet-client` looks for scripts to execute at boot and every 5 minutes, and therefore execution is not instantaneous.

13.7 Configuration for the use of OCS inventory agent.

The agent can be installed on the physical machines (thus proxmox and the clients) within a school's network. The agent is installed on the clients automatically by `fuss-client` (starting with version 11.0.22 for Fuss 11, 12.0.7 for Fuss 12) either when connecting the client to the server, or when upgrading. It is ne- cessary that the correct configuration be present on the FUSS server, to be set up in the manner we will explain later.

To install it on Proxmox, or on any other (Debian) machine that can be reached by the FUSS Server, it will be necessary instead to run on it the `ocs-agent-inst` playbook (installed in `/usr/share/fuss-server/`) that comes with the `fuss-server` package starting with version 12.0.10. The script is also usable for a client, but it is preferable to avoid its use, since the configuration is still generated by `fuss-client`, in a slightly different way, to be automatically updatable by future versions of the package.

In order to function, the agent needs to reach via the network the machine on which the OCS inventory server is hosted; this is contacted via the web and therefore it is necessary as a first step to enable its reachability. This must be done preliminarily on the FUSS server by adding an appropriate ac- cess rule for the proxy, allowing it to reach the OCS inventory server without the need for authentication; for this purpose it will be sufficient to add to the `/etc/squid/squid-added-repo.conf` file the line:

```
acl repositories url_regex ocs.inventory.server
```

where `ocs.inventory.server` is the address of the OCS inventory server you intend to use. After the change you will have to perform a reload of `squid` with `systemctl reload squid`.

The next step involves:

- (if the server certificate is self-signed), download it from the site, name it `server.crt` and copy it to the FUSS server in the `/var/www/fuss-data-conf/` folder.
- create in the same folder the file `ocsinventory.yml` (with YAML syntax) containing the configuration parameters to be used later on the clients. This file will then be downloaded to each client when the `fuss-client` is launched.

The file requires the definition of three variables, the first two are mandatory, the third is optional:

- `ocs_server` : the indication of the server URL, e.g. https://ocs.inventory.server/ocsinventory
- `ocs_tag` : the tag that identifies the school, e.g. the (LASIS) numeric school code

- **ocs_cert** [(optional) the name of the certificate to be used for] the SSL connection (needed only if the server has a self-signed certificate); if defined said file must be installed under `/var/www/fuss-data-conf/` .

An example of this file is as follows:

```
# template for ocsinventory variables needed for fuss-
client ocs_server:
https://ocs.inventory.server/ocsinventory ocs_tag: change-
me
ocs_cert: server.crt
```

To prevent an update performed on a client during configuration from finding a partially written `ocsinventory. yml` file, resulting in errors, it is suggested that it be created in another directory, moving it to desti- nation once complete (along with the certificate file previously uploaded to the server, when necessary) with:

```
mv ocsinventory.yml /var/www/fuss-data-conf/
```

Note: It i s recommended, if possible, to configure the OCS inventory server with a valid certificate (e.g., using Let's Encrypt) while avoiding the use of a self-signed certificate; in that case the `ocs_cert` variable is not needed, as is the certificate.

At this point, simply run `fuss-client to` install the agent. The configuration file (`ocsinventory.yml`), when present, is downloaded in the execution of the command (both when su uses `-a` or `-H` to connect a new client, than when using `-U` for an upgrade), and is saved in `/ etc/fuss-client/`. When that file is found, the configuration and installation of `ocsinventory-agent` is then performed. If, however, the file is not found on the server, the program continues without installing anything.

In case you forgot to copy the `server.crt` certificate to the FUSS server before launching `fuss-client`, you can correct the problem (after copying the certificate to the server) by re-launching the `fuss-client -U` command.

13.7.1 Installing ocs agent on a generic (non-joined) machine

To install the agent on a generic machine, one can instead use the `ocs-agent-inst` playbook found on the FUSS server. This performs the installation of `ocsinventory-agent` on a generic machine to be designated as part of the inventory That is, the command must be run on the FUSS server as:

```
/usr/share/fuss-server/scripts/ocs-agent-inst -i <client.address.or.ip>,
```

taking care to put a comma after the client address so that it is recognized as a list of addresses and not as a file name.

Keep in mind that the playbook `requires` access via SSH to the indicated machine; if you `do` not have direct key access, you will need to request the use of the (root) password by adding the `-K` option.

CHAPTER 14

Idea Incubator

This section represents a small showcase of incubating ideas and proposals that have yet to be thoroughly tested. They are intended to give the opportunity

- to anyone with proposals, to see them published after an initial round of approval by the project team;
- to anyone who wants to, to view and/or test these proposals by adding their comments on the mailing list **fuss-devel** https://www.fuss.bz.it/cgi-bin/mailman/listinfo/fuss-devel.

14.1 Proposal 1: Installation of FUSS Server starting from Debian Cloud upstream

Author: Marco Marinello

If you want to quickly install a virtualized server from an up-to-date version of Debian, the best choice is definitely to start from a disk provided directly by Debian.

By going to https://cloud.debian.org/images/cloud/ you can see a list of available cloud images. Choose the one related to the current server distro (`buster` at the moment) then the penultimate entry, before `daily`, which is the last stable one. Among the various files listed, copy the link of `generic-amd64-*.qcow2`, connect to the Proxmox server that is to host it and, after creating the virtual machine, run

```
cd /opt
wget https://cloud.debian.org/images/cloud/buster/20201023-432/debian-10-generic-
↪amd64-20201023-432.qcow2
# Import the disk on the local-lvm storage for the machine with ID 100.
qm importdisk 100 debian-10-generic-amd64-20201023-432.qcow2 local-lvm
```

At this point remove the old disk (which was automatically created by the wizard) from the VM through the Proxmox GUI and "plug in" the new one. Extend the disk (usually the template consists of 2GB so it is advisable to increase by at least 48 to get to 50GB of root) and add a second one to be used later for home. Add a serial port, the necessary network ports and a Cloud-Init volume. Once the "Cloud-Init" tab has been properly enhanced, it will be sufficient to start the VM for Cloud-Init to perfect the configuration. Once the machine is booted wait for unattended-upgrades to install the updates then run

```
fdisk /dev/sdb
# n
# p
# 1
# <enter>
# <enter>
# w
mkfs.ext4 /dev/sdb1
# Enable disk controls tune2fs
-c 50 -i 30d /dev/sda1 tune2fs
-c 50 -i 30d /dev/sdb1 blkid
```

Use the result of blkid to value the `/etc/fstab` file. Also replace the last two values in the root disk with *1 0* and use *1 1* for the disk with the home instead. Finally, run `mount -a` and verify through the `df -h` command that the disk has been mounted correctly.

You can now proceed to the removal of Cloud-Init (which would only create mischief from now on) and the actual configuration:

```
apt purge cloud-init
mv /etc/network/interfaces.d/50-cloud-init /etc/network/interfaces
apt install gnupg2 qemu-guest-agent nfs-common
apt install -t buster-backports ansible systemd
wget -O - https://archive.fuss.bz.it/apt.key | apt-key add
- sed -i 's/main/main contrib/g' /etc/apt/sources.list
echo 'deb http://archive.fuss.bz.it/ buster main contrib' >> /etc/apt/sources.list
apt update
apt install fuss-server fuss-backup
```

14.2 Proposal 2: Soft migration from FUSS 8 server to FUSS 10 server.

Author: Marco Marinello

In order to simplify the migration of schools from the eighth version of FUSS Server and Client to the tenth, it is possible to break the migration into two. You can migrate server and client separately; the order does not matter. This guide applies to all of the following contexts:

- FUSS 8 server and FUSS 8 client
- FUSS 8 server and FUSS 9 client
- FUSS 8 server and FUSS 10 client

14.2.1 Backing up the old server

As a first step, be sure to "take away" all data essential to the migration. It is assumed `fuss-backup` is already configured and operational. If it is not, follow the relevant guide. Check in the `/etc/ fuss-backup/fuss-backup.conf` file that the `PATHS` variable is correctly valued and add `/ root` and the other directories you want to back up.

```
PATHS="/etc /home /var/backups /var/lib /var/log /var/mail /var/local /root /srv"
```

From now on, the network is assumed to be unloaded (there should be no operations running or users logged on). Therefore, go back to the root home and run

```
slapcat > dump_pre_mig.ldif
```

which will generate a backup of LDAP in the file

`/root/dump_pre_mig.ldif` . Then run, to create a backup of the

```
octofussctl -u root http://localhost:13400/conf > groups_backup.txt <<EOF
ls users/groups
EOF
```

groups

Clean up the file by removing the first line "Welcome to the octofussd client [. . .]", the first and last />. You then execute

```
sed -i 's+^+create users/groups/+' groups_backup.txt
```

so that the file is ready for import into the new server.

Move this file in addition to `/root/dump_pre_mig.ldif` and `/etc/fuss-backup/fuss-backup.conf` to your machine then run `fuss-backup` . If `root` is among the recipients you will be able to check the outcome of the backup with the `mail` command. You will also note down the *SSH* keys authorized for access and the IPs of the machine. The new server should be *identical* to the old one, nothing can be changed between IP, domain name, server hostname and root password.

14.2.2 Installation of the new server

Start by installing fuss-server using any of the methods given on this guide. Here we go on to intend that `fuss-server` is installed along with `fuss-backup` but has never been run.

You start by mounting the resource that was backed up from the old server. You can verify this from the `fuss-backup.conf` copied just now.

```
mount 172.16.11.22:/myback /mnt
```

You can now proceed to extract some files necessary for continuation (we assume you are working as `root`):

```
cd
mkdir from_backup cd
from_backup
borg extract --progress /mnt/borgdata::$(borg list /mnt/borgdata|tail -1|cut -d '
↪' -f 1) etc/fuss-server etc/fuss-backup etc/fuss-server etc/fuss-backup var/lib/
↪krb5kdc/principal etc/krb5kdc etc/krb5.keytab root
```

You then copy the old `fuss-server.yaml` file in-place and run `fuss-server`. If the host configuration is the same as before, there should be no errors and no questions should be asked. If it does, check the correctness of the configuration done so far. If the captive portal was configured, you can reconfigure it right away, subject to ascertaining the network file requirements as described in the relevant guide.

```
cp etc/fuss-sevrer/fuss-server.yaml /etc/fuss-
server fuss-server create
# Per captive portal (if required) - check interface correspondence.
cp etc/fuss-server/fuss-captive-portal.conf /etc/fuss-
server fuss-server cp
```

A reboot is recommended at this point to make sure everything is working.

Importing users

Warning: Be sure that the version of octonet is >= 10.0.4-2 and octofussd >= 10.0.15-1

Creation of groups

In order not to run into errors, first you recreate the groups you had on the old server. The fi- le groups_backup.txt should have been extracted from the backup in /root/from_backup/root/groups_backup.txt

```
octofussctl -u root http://localhost:13400/conf < /root/from_backup/root/groups_
↪backup.txt
```

LDIF file conversion from OctoNet

Connect from your machine to OctoNet via browser and log in. You then go to *Users and Groups* > *Convert LDIF file*. Upload the previously exported file and download the output to CSV. You then edit the CSV file with LibreOffice and remove the *password* column that contains automatically generated ones and save.

Importing the new CSV

Now that you have the list of users you can import these into the new server. Again from *Users and Groups* choose *Import from CSV*. Load the CSV file you just prepared, select the first row (header) to make it ignored, and associate the columns. Make sure you have associated the *Hashed password* otherwise the users will be created without a password. Allow the import and wait patiently for it to finish. The progress bar should signal the progress of the operation.

Now all users should have been recreated with their (empty) homepages.

Restoring Kerberos Files

Once all users have been created, the old Kerberos files with credentials can be moved in-place.

```
systemctl stop octofussd octonet fuss-manager krb5-admin-server krb5-kdc nfs-
↪common nfs-kernel-server cp
/etc/krb5.keytab{,-fs_old}
cp /var/lib/krb5kdc/principal{,-fs_old}
cp /root/from_backup/etc/krb5.keytab /etc/.
cp /root/from_backup/var/lib/krb5kdc/principal /var/lib/krb5kdc/
```

Reboot the server now to return to a clean situation from the services point of view. You can now turn on a client and try logging in with an imported user. If everything has been done correctly, you should log in and see your (empty) home.

Home extraction

The last step is to restore the home from the backup. Since this is a lengthy process, it is advisable to perform it in screen.

```
cd /
borg extract --progress /mnt/borgdata::$(borg list /mnt/borgdata|tail -1|cut -d '
↪' -f 1) home
```

Configuring the new backup

When reconfiguring `fuss-backup`, it is advisable not to use the `borgdata` directory again so as not to affect the old backup. Rather, something like `borgdata10 should` be preferred.

Restoring other data or previous configurations

The server should now be fully operational. However, you can restore additional data (such a s clonezilla images) or configurations (such as firewall configurations) from the backup.

These are left as an exercise for the reader.

CHAPTER 15

Contribute

Anyone can help improve this documentation that is written in reStructuredText.

15.1 Authors

The following people participated in the writing of this guide.

- Paul Baratta
- Claudio Cavalli
- Piergiorgio Cemin
- Paul Dongilli
- Donato Florio
- Elena Grandi, Truelite Srl
- Marco Marinello
- David Noble
- Andrea Padovan
- Simone Piccardi, Truelite Srl
- Michael Von Guggenberg

Details and contribution history are available on the git repository.

CHAPTER 16

Support

If you need help, email info@fuss.bz.it

CHAPTER 17

Licenses



