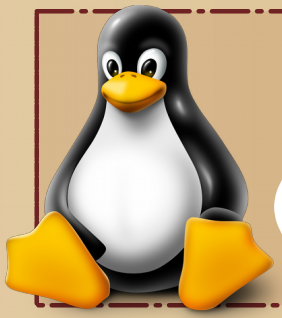
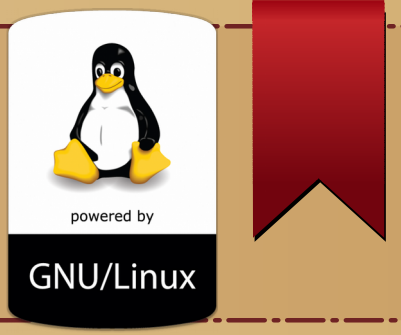


La Sicurezza
(Vista dal “pinguino” e non solo)



“Percorso tra i vari aspetti della Sicurezza (principalmente in GNU/Linux”)

creative commons

Sicurezza
Cosa s’intende?

- Vandalismo? No

- Condizioni di sicurezza sul lavoro o dove abitate? No. Ma ad esempio il DPS (Documento Programmatico della Sicurezza), a livello legislativo, serve per tutelare anche i dati di altre persone, non solo di voi stessi.

Privacy
Cosa s’intende?

“Non mi preoccupo perché non ho niente da nascondere...”

(Siete contrabbandieri? Falsari? Trafficanti di droga? No. Avete sempre e comunque diritto alla vostra sicurezza e la vostra privacy)

Edward Joseph Snowden (Elizabeth City, 21 giugno 1983) è un informatico e attivista statunitense.

Ex tecnico della CIA e fino al 10 giugno 2013 collaboratore della Booz Allen Hamilton (azienda di tecnologia informatica consulente della NSA, la National Security Agency), è noto per aver rivelato pubblicamente dettagli di diversi programmi di sorveglianza di massa del governo statunitense e britannico, fino ad allora tenuti segreti.

Sistemi Operativi ?

Quale sistema operativo è sicuro?

- Windows
- Linux
- Mac OS X
- As/400 .. LOL 

Questo SI …
… che è un computer sicuro!!

OpenSource è sicuro?

Comprereste un'auto con il cofano sigillato?

OpenSource è sicuro?
Vantaggi e svantaggi

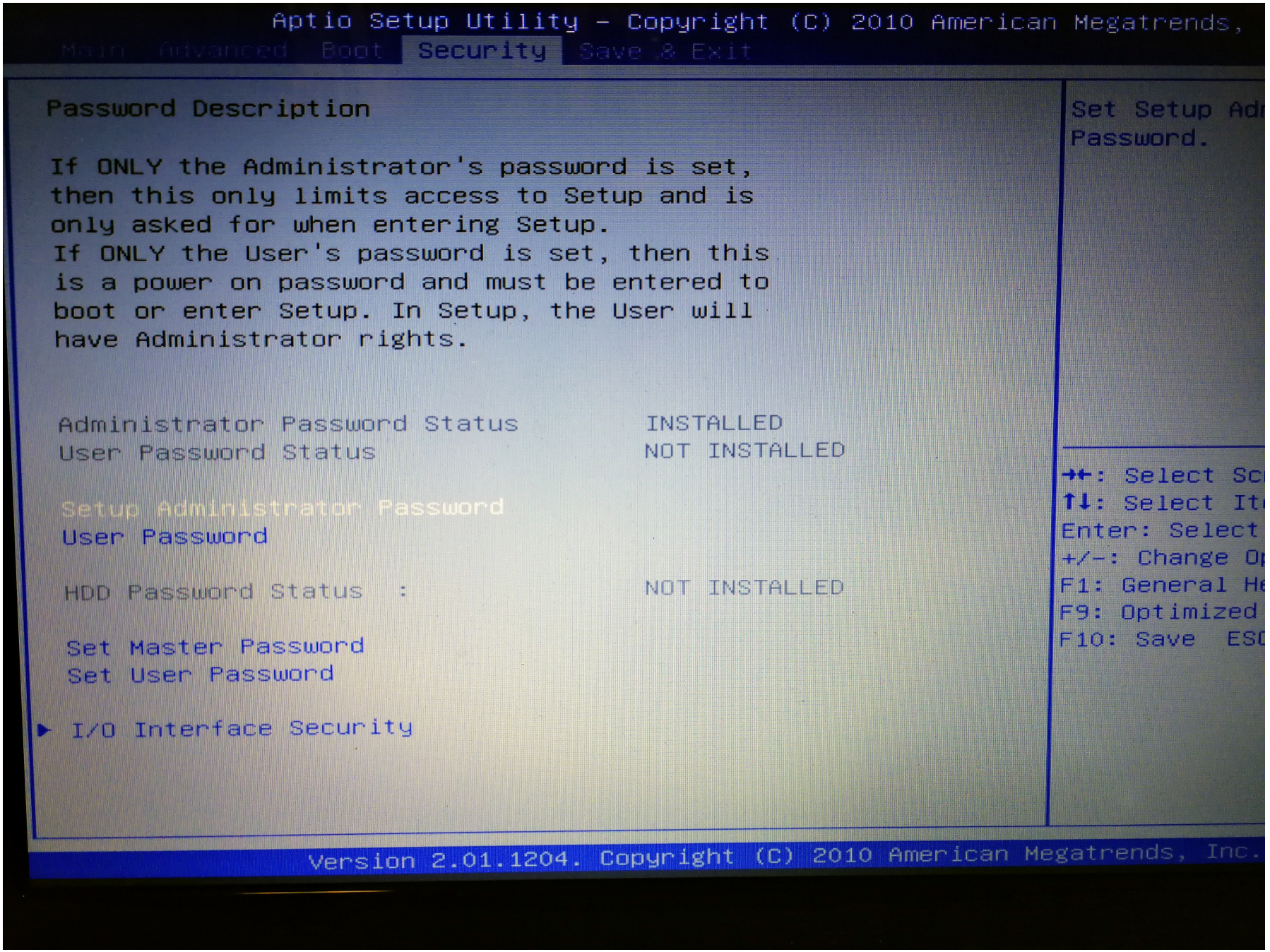
Vantaggi

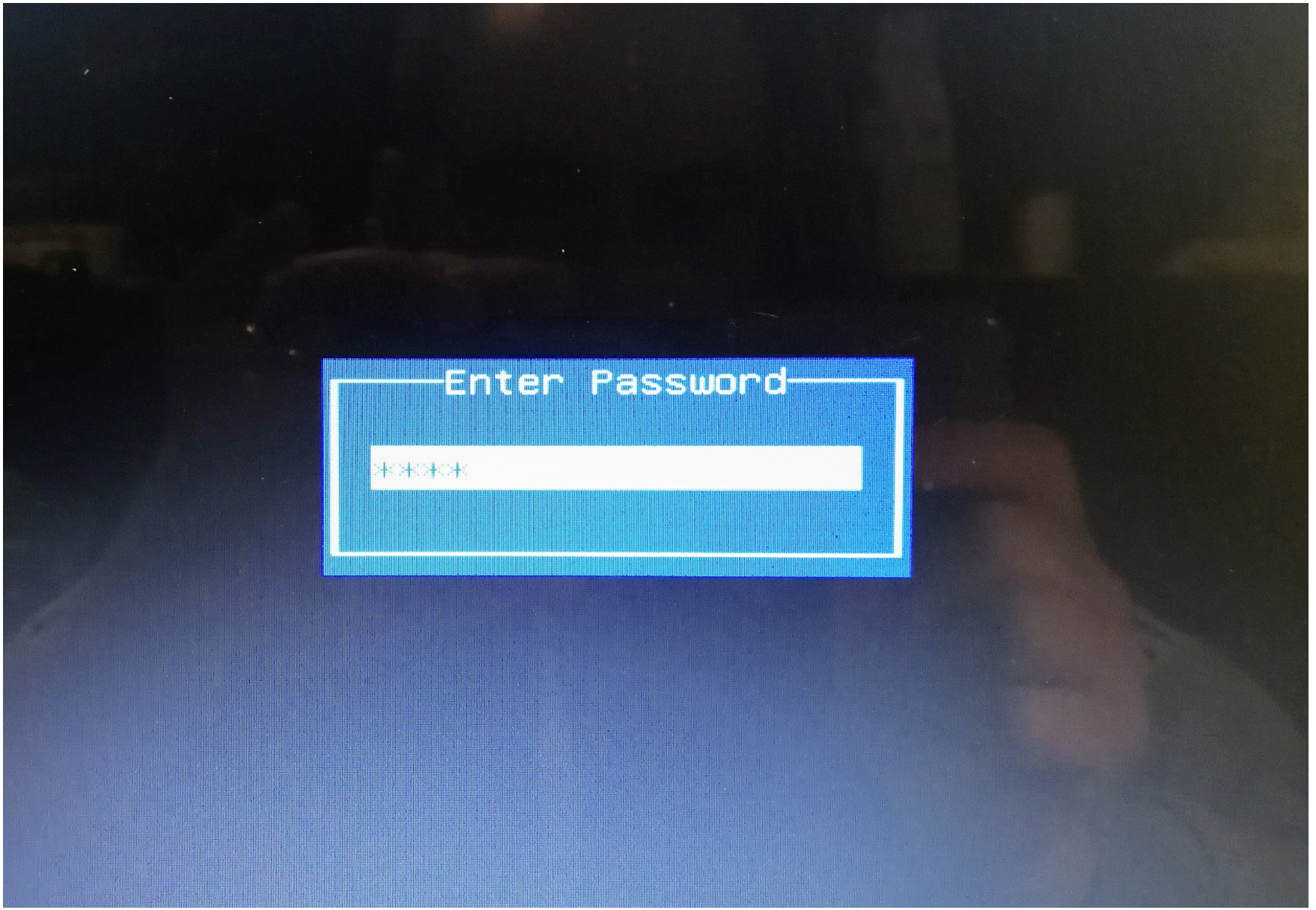
- Presenza di CVE (Common Vulnerabilities and Exposures) aggiornati (https://cve.mitre.org .. https://www.cvedetails.com .. italiano https://www.certnazionale.it/bollettini/)
- Estesa comunità al lavoro, in continuo miglioramento.

Svantaggi

- Opensource agli occhi di tutti, può essere d'altro canto usato per trovare più facilmente backdoors (**hacker** di cattiva fede)...
- (TESI COMPLOTTISTICA: Multinazionali antivirus e/o Software commerciale/ Sistemi proprietari, possono impiegare esperti per studiare il codice e boicottare l'OpenSource a proprio vantaggio)

BIOS Password




Enter Password

Mettere il GRUB in sicurezza.

(GNU GRand Unified Bootloader)

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Modifica Visualizza Cerca Terminale Aiuto

```
root@debianstable:/etc/grub.d# ls -la
totale 92
drwxr-xr-x   2 root root  4096 dic  5 14:41 .
drwxr-xr-x 185 root root 12288 dic  5 14:48 ..
-rwxr-xr-x   1 root root  9783 feb 11  2017 00_header
-rwxr-xr-x   1 root root  6258 feb 11  2017 05_debian_theme
-rwxr-xr-x   1 root root 12455 nov 21 17:48 10_linux
-rwxr-xr-x   1 root root 11281 feb 11  2017 20_linux_xen
-rwxr-xr-x   1 root root 12059 feb 11  2017 30_os-prober
-rwxr-xr-x   1 root root  1418 feb 11  2017 30_uefi-firmware
-rwxr-xr-x   1 root root   540 nov 21 17:35 40_custom
-rwxr-xr-x   1 root root   216 dic 12  2013 41_custom
-rw-r--r--   1 root root   483 lug  3  2013 README
root@debianstable:/etc/grub.d# grub-mkpasswd-pbkdf2   ####### (Password-Based Key Derivation Function 2)
Inserire la password:
Reinserire la password:
L'hash PBKDF2 della password è grub.pbkdf2.sha512.10000.60501DF4A95203674F4D733AE0FE2E32CE7543F364FF096A12CB89F9F6EFF9DB80E2FC752D1E6870EF
D9DB26FA2F7D46D8DE0D136EAC897D92E5139522411102.800A81B9D9578A927B887E91F41C8384DAB9059CC204DB37C560CF403421707ED062FCBC4E7CFA3FC6EB5CE72AF
FEB79796E4DFCA93D6025B0674E4D2706309A
root@debianstable:/etc/grub.d# vi -o 40_custom 10_linux
2 file da elaborare
```

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Modifica Visualizza Cerca Terminale Aiuto

```
#!/bin/sh
exec tail -n +3 $0
# This file provides an easy way to add custom menu entries.  Simply type the
# menu entries you want to add after this comment.  Be careful not to change
# the 'exec tail' line above.
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.10000.60501DF4A95203674F4D733AE0FE2E32CE7543F364FF096A12CB89F9F6EFF9DB80E2FC752D1E6870EFD9DB26FA2F
7D46D8DE0D136EAC897D92E5139522411102.800A81B9D9578A927B887E91F41C8384DAB9059CC204DB37C560CF403421707ED062FCBC4E7CFA3FC6EB5CE72AFFEB79796E4
DFCA93D6025B0674E4D2706309A
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
40_custom                                                                    7,22          Tut
      esac
      if [ x"$title" = x"$GRUB_ACTUAL_DEFAULT" ] || [ x"Previous Linux versions>$title" = x"$GRUB_ACTUAL_DEFAULT" ]; then
          replacement_title="$(echo "Advanced options for ${OS}" | sed 's,>,>>,g')>$(echo "$title" | sed 's,>,>>,g')"
          quoted="$(echo "$GRUB_ACTUAL_DEFAULT" | grub_quote)"
          title_correction_code="${title_correction_code}if [ \"x\$default\" = '$quoted' ]; then default='$(echo "$replacement_title" | gr
ub_quote)'; fi;"
          grub_warn "$(gettext_printf "Please don't use old title \`%s' for GRUB_DEFAULT, use \`%s' (for versions before 2.00) or \`%s' (f
or 2.00 or later)" "$GRUB_ACTUAL_DEFAULT" "$replacement_title" "gnulinux-advanced-$boot_device_id>gnulinux-$version-$type-$boot_device_id"
)"
      fi
      echo "menuentry '$(echo "$title" | grub_quote)' --unrestricted ${CLASS} \$menuentry_id_option 'gnulinux-$version-$type-$boot_device_
id' {" | sed "s/^/$submenu_indentation/"
  else
      echo "menuentry '$(echo "$os" | grub_quote)' --unrestricted ${CLASS} \$menuentry_id_option 'gnulinux-simple-$boot_device_id' {" | se
d "s/^/$submenu_indentation/"
  fi
  if [ "$quick_boot" = 1 ]; then
      echo "    recordfail" | sed "s/^/$submenu_indentation/"
  fi
  if [ x$type != xrecovery ] ; then
      save_default_entry | grub_add_tab
  fi
10_linux                                                                     132,53         35%
-- VISUALE RIGA --                                                                    1
```

Ctrl destro

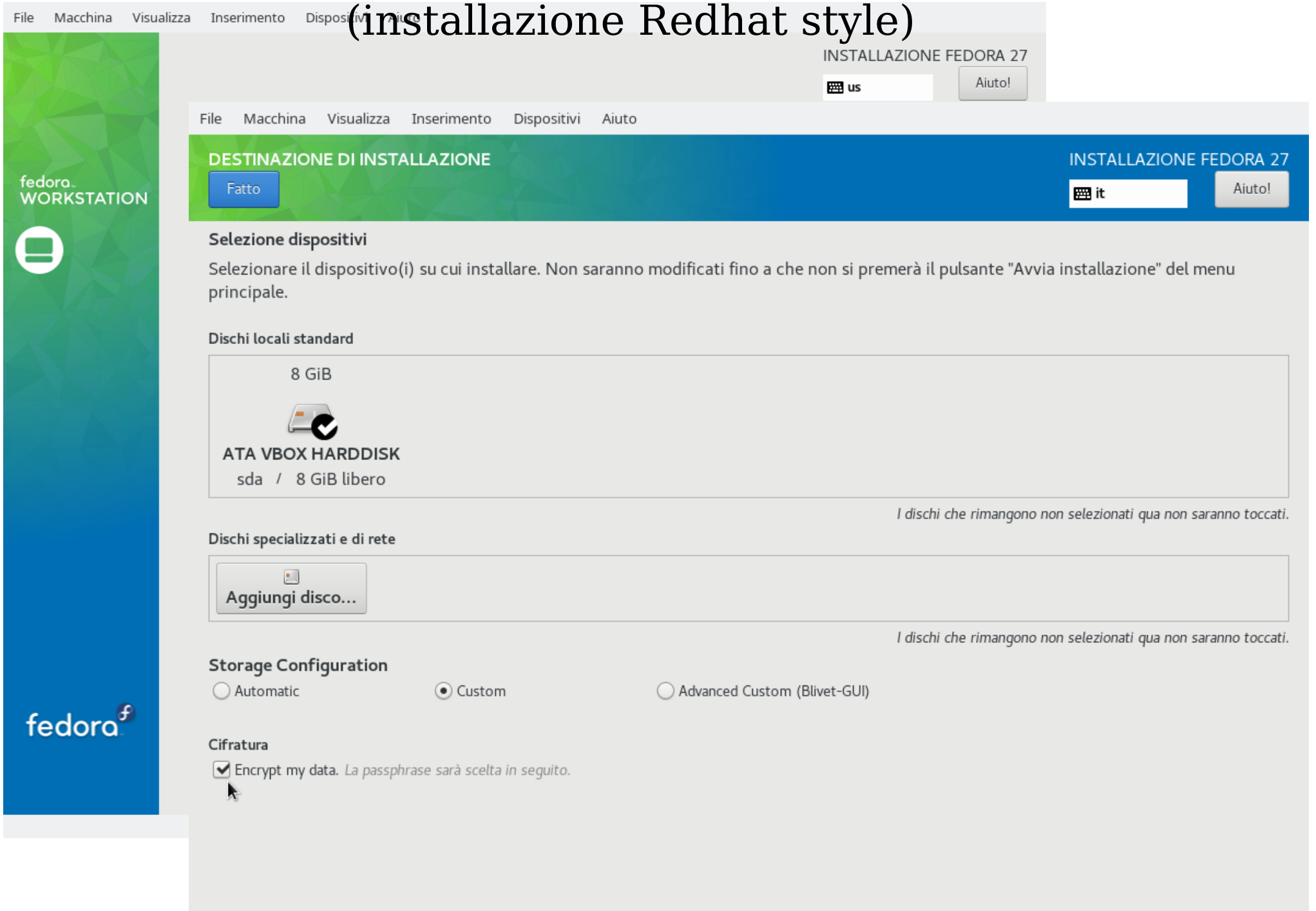
```
root@debianstable:/etc/grub.d# update-grub
update-grub   update-grub2
root@debianstable:/etc/grub.d# grub-mkconfig -o /boot/grub/grub.cfg
Generazione file di configurazione GRUB...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Trovata immagine linux: /boot/vmlinuz-4.9.0-4-amd64
Trovata immagine initrd: /boot/initrd.img-4.9.0-4-amd64
Trovata immagine linux: /boot/vmlinuz-4.9.0-3-amd64
Trovata immagine initrd: /boot/initrd.img-4.9.0-3-amd64
fatto
root@debianstable:/etc/grub.d#
```

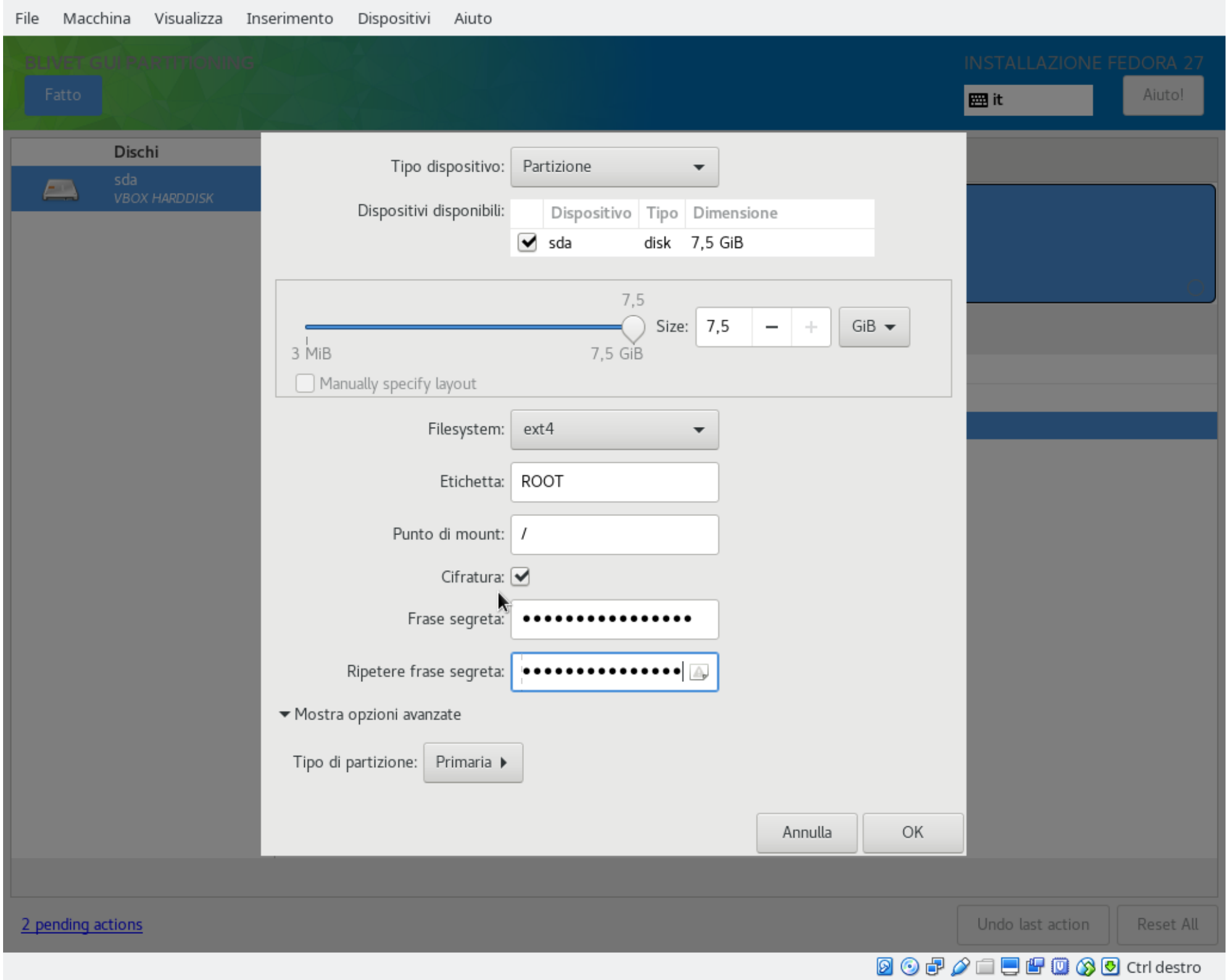
GRUB2 - un esempio tipico di *grub.cfg* una volta creata la configurazione:

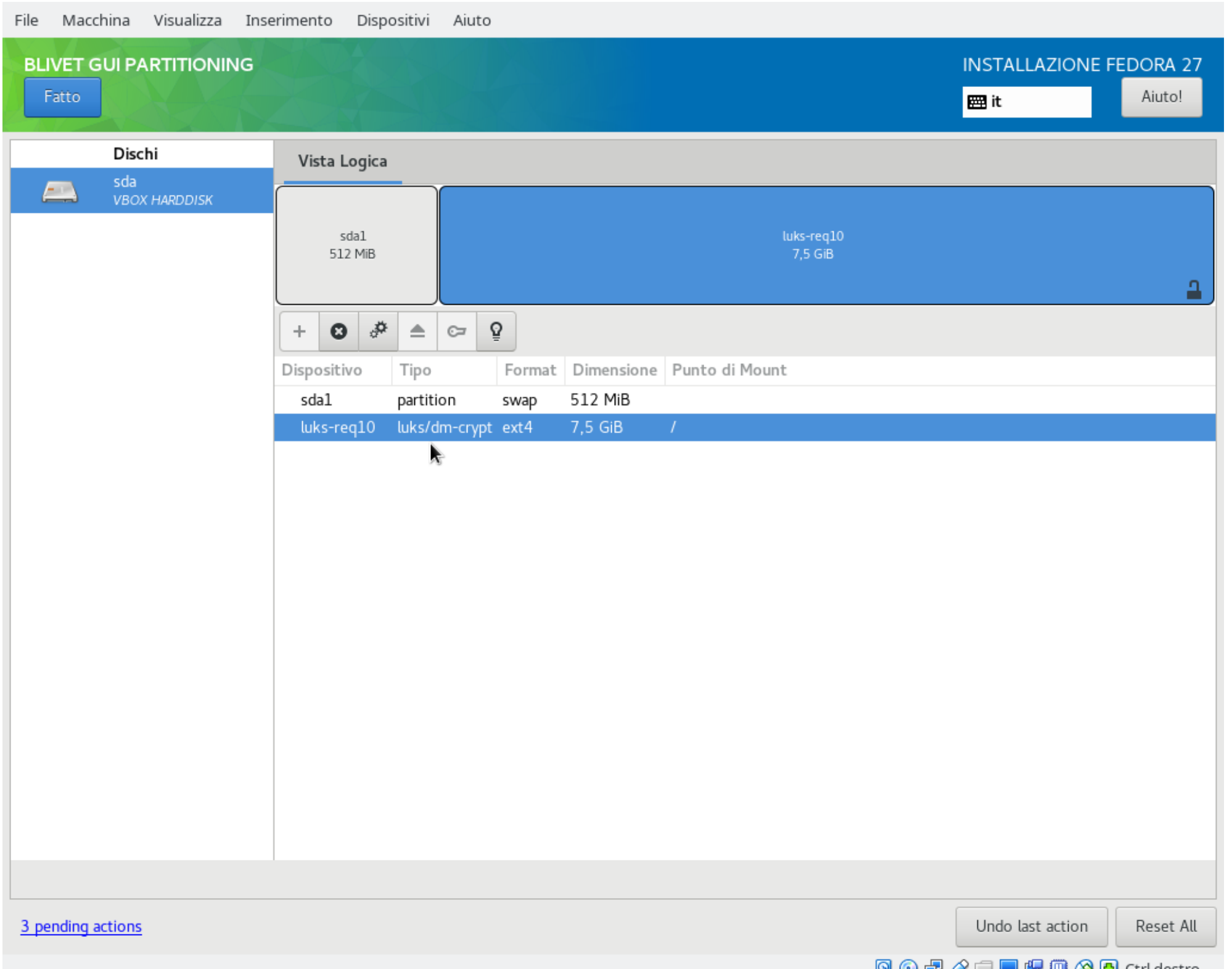
```
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.10000.biglongstring
password user1 insecure
 …..
menuentry "May be run by any user" --unrestricted {
   set root=(hd0,1)
   linux /vmlinuz
}
 ….
menuentry "Superusers only" --users "" {
   set root=(hd0,1)
   linux /vmlinuz single
}

menuentry "May be run by user1 or a superuser" --users user1
{
   set root=(hd0,2)
   chainloader +1
}
 ….
```

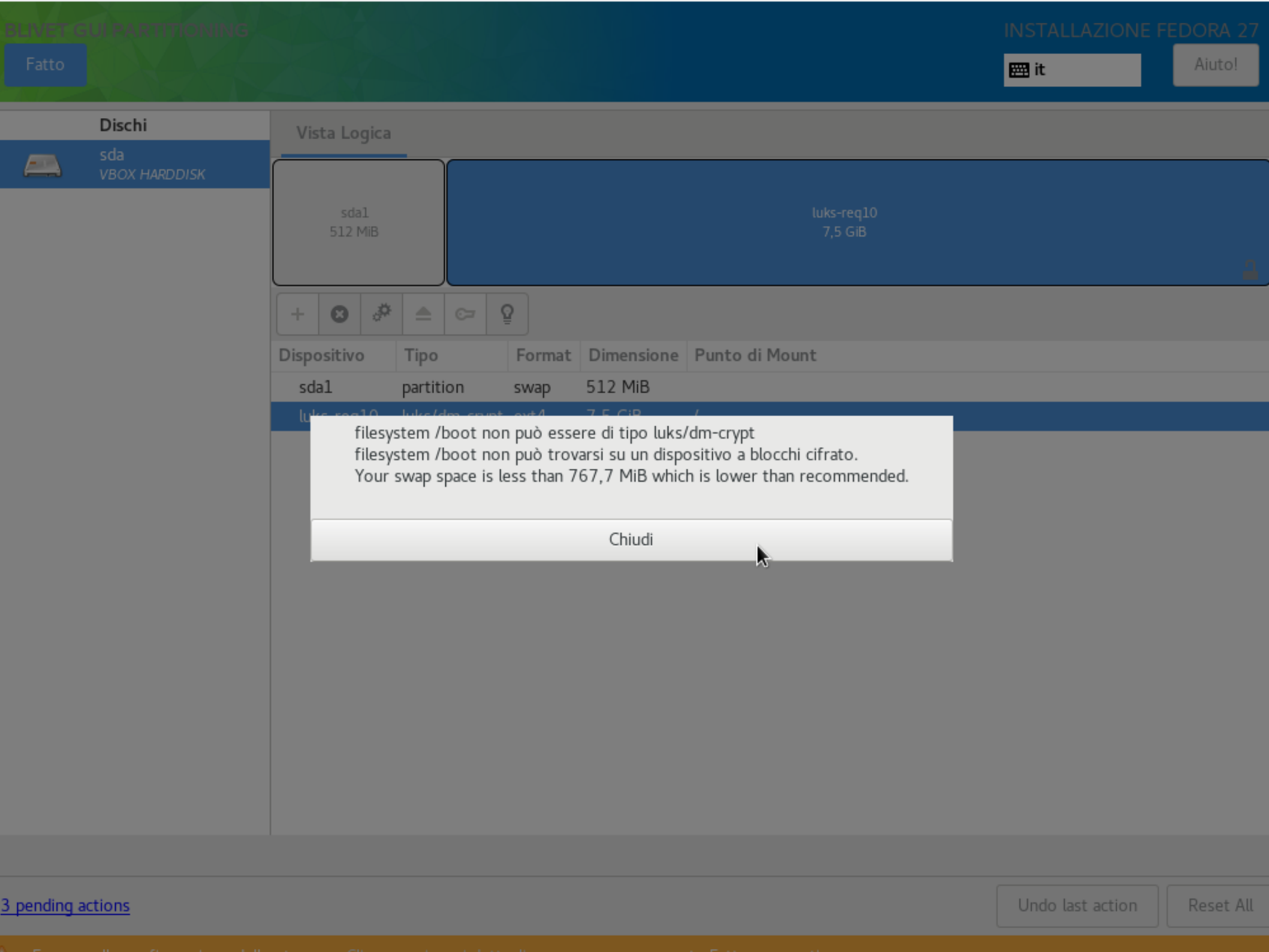
Encrypted Filesystem

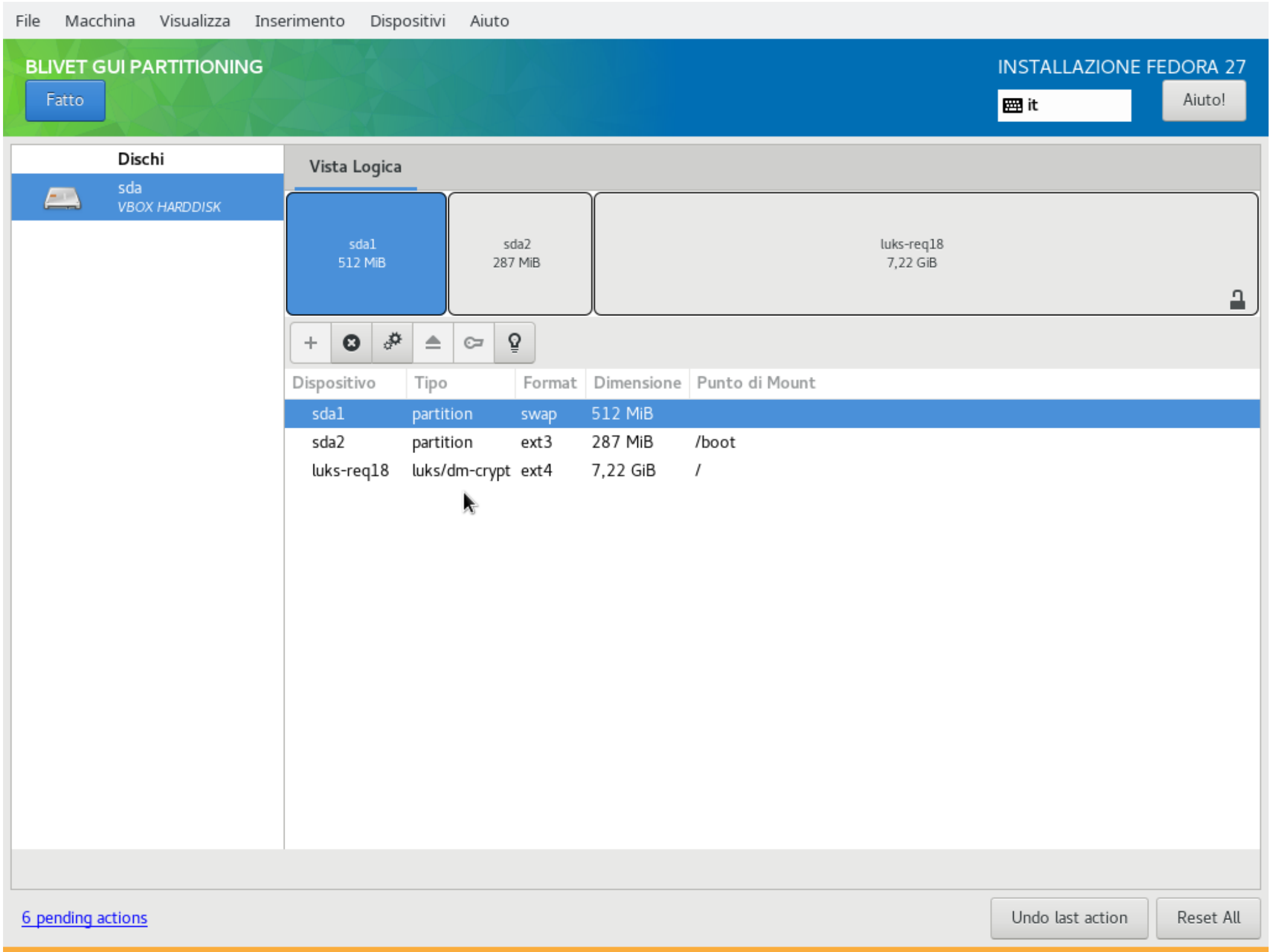
(installazione Redhat style)

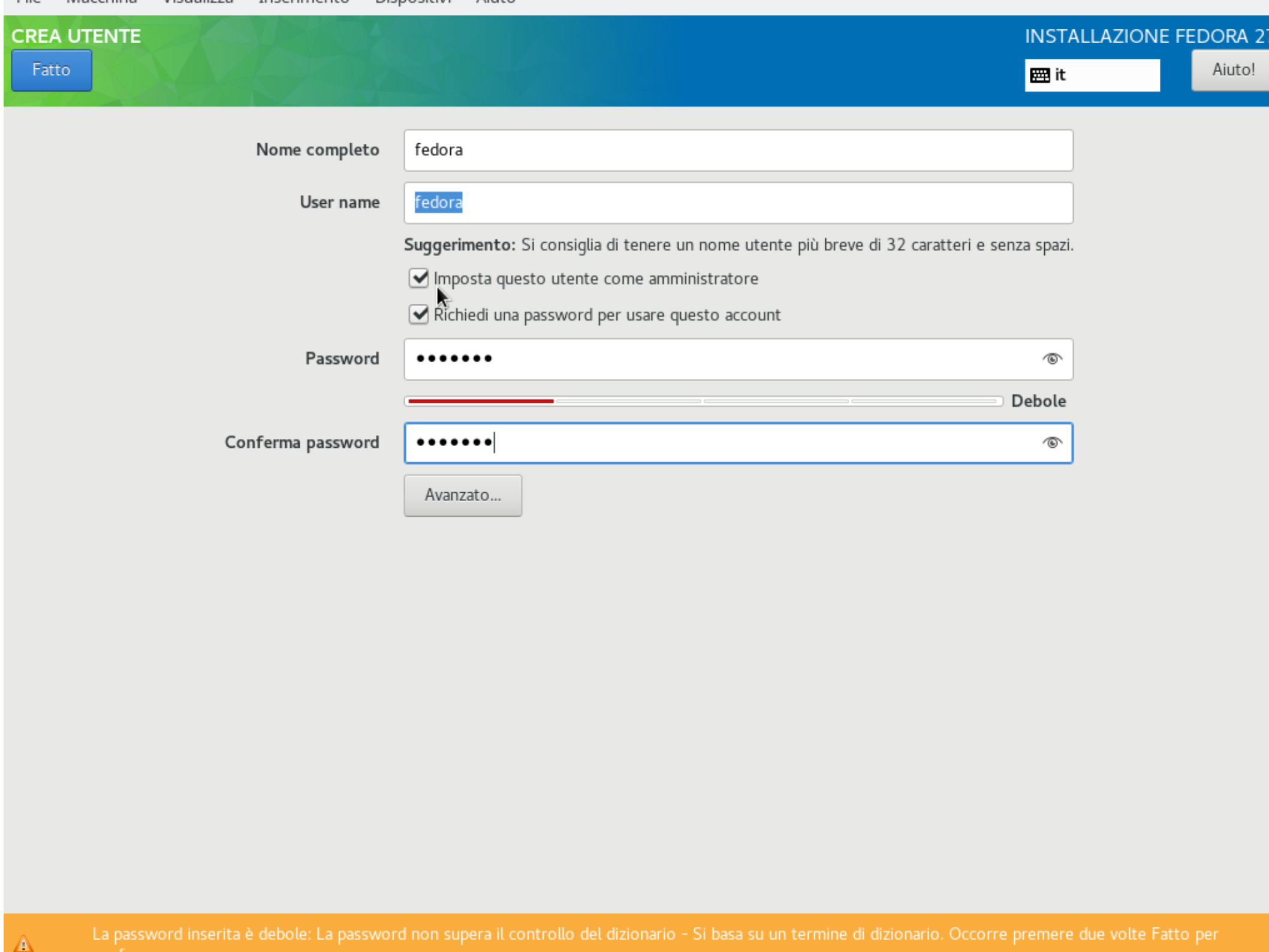


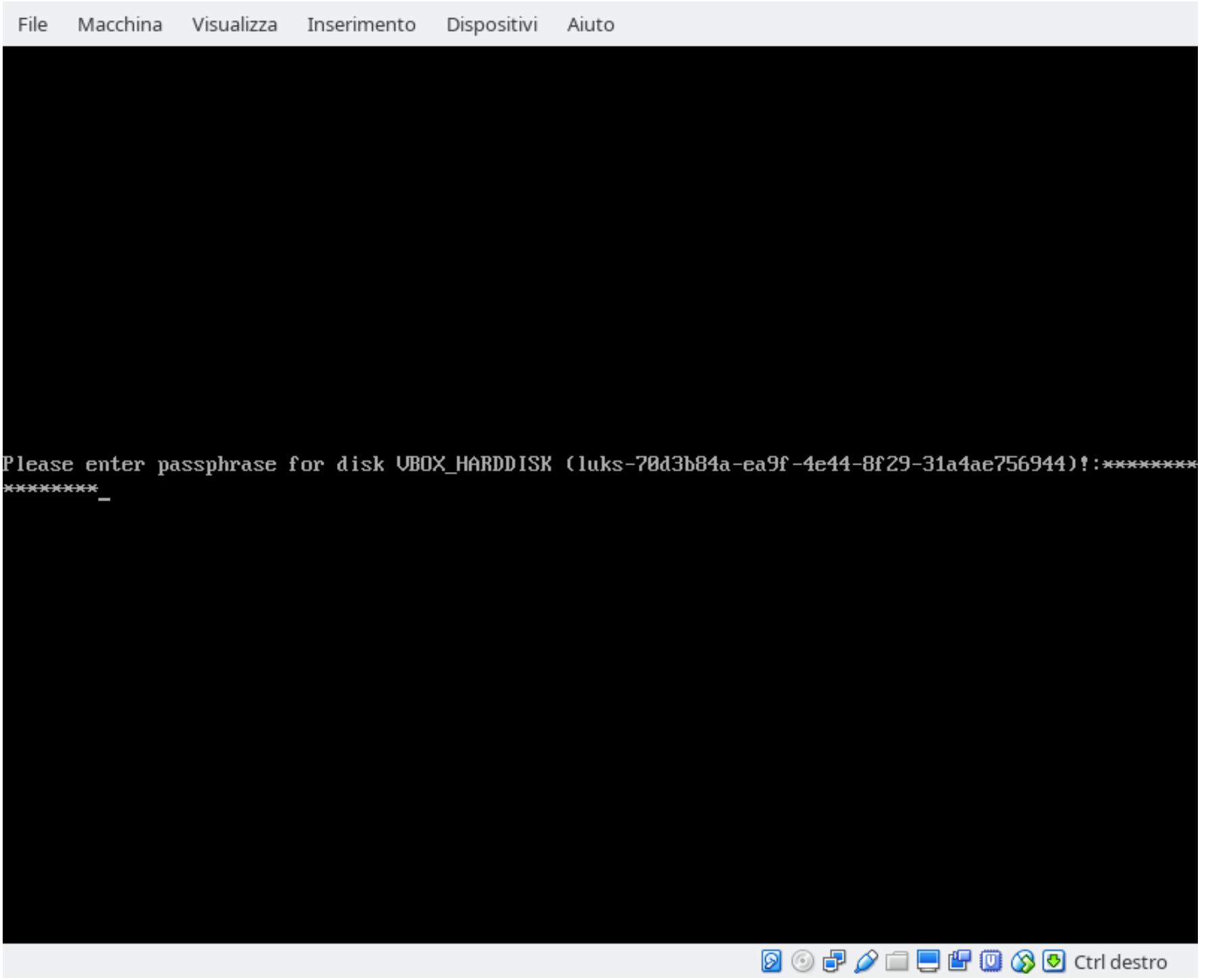

File Macchina Visualizza Inserimento Dispositivi Aiuto
BLIVET GUI PARTITIONING
Fatto
INSTALLAZIONE FEDORA 27
it
Aiuto!
Dischi
sda
VBOX HARDDISK
Tipo dispositivo: Partizione
Dispositivi disponibili:
Dispositivo Tipo Dimensione
sda disk 7,5 GiB
7,5
Size: 7,5 GiB
3 MiB
7,5 GiB
Manually specify layout
Filesystem: ext4
Etichetta: ROOT
Punto di mount: /
Cifratura:
Frase segreta:
Ripetere frase segreta:
Mostra opzioni avanzate
Tipo di partizione: Primaria
Annulla
OK
2 pending actions
Undo last action
Reset All
Ctrl destro

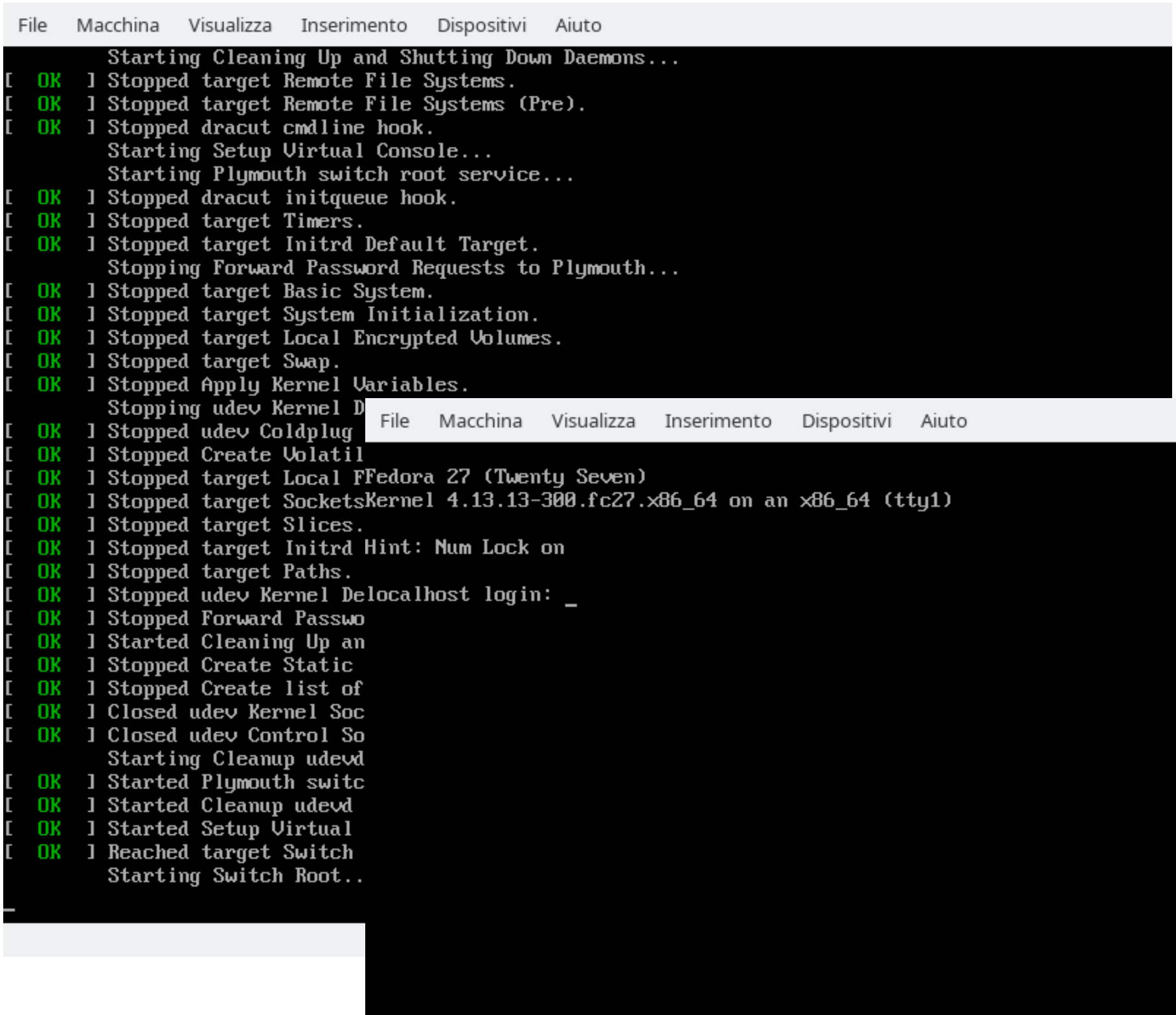

File Macchina Visualizza Inserimento Dispositivi Aiuto
BLIVET GUI PARTITIONING
Fatto
INSTALLAZIONE FEDORA 27
it
Aiuto!
Dischi
sda
VBOX HARDDISK
Vista Logica
sda1
512 MiB
luks-req10
7,5 GiB
Dispositivo Tipo Format Dimensione Punto di Mount
sda1 partition swap 512 MiB
luks-req10 luks/dm-crypt ext4 7,5 GiB /
3 pending actions
Undo last action
Reset All


BLIVET GUI PARTITIONING
INSTALLAZIONE FEDORA 27
Fatto
it
Aiuto!
Dischi
sda
VBOX HARDDISK
Vista Logica
sda1
512 MiB
luks-req10
7,5 GiB
Dispositivo
Tipo
Format
Dimensione
Punto di Mount
sda1
partition
swap
512 MiB
filesystem /boot non può essere di tipo luks/dm-crypt
filesystem /boot non può trovarsi su un dispositivo a blocchi cifrato.
Your swap space is less than 767,7 MiB which is lower than recommended.
Chiudi
3 pending actions
Undo last action
Reset All


File Macchina Visualizza Inserimento Dispositivi Aiuto
BLIVET GUI PARTITIONING
Fatto
INSTALLAZIONE FEDORA 27
it
Aiuto!
Dischi
sda
VBOX HARDDISK
Vista Logica
sda1
512 MiB
sda2
287 MiB
luks-req18
7,22 GiB
Dispositivo Tipo Format Dimensione Punto di Mount
sda1 partition swap 512 MiB
sda2 partition ext3 287 MiB /boot
luks-req18 luks/dm-crypt ext4 7,22 GiB /
6 pending actions
Undo last action
Reset All

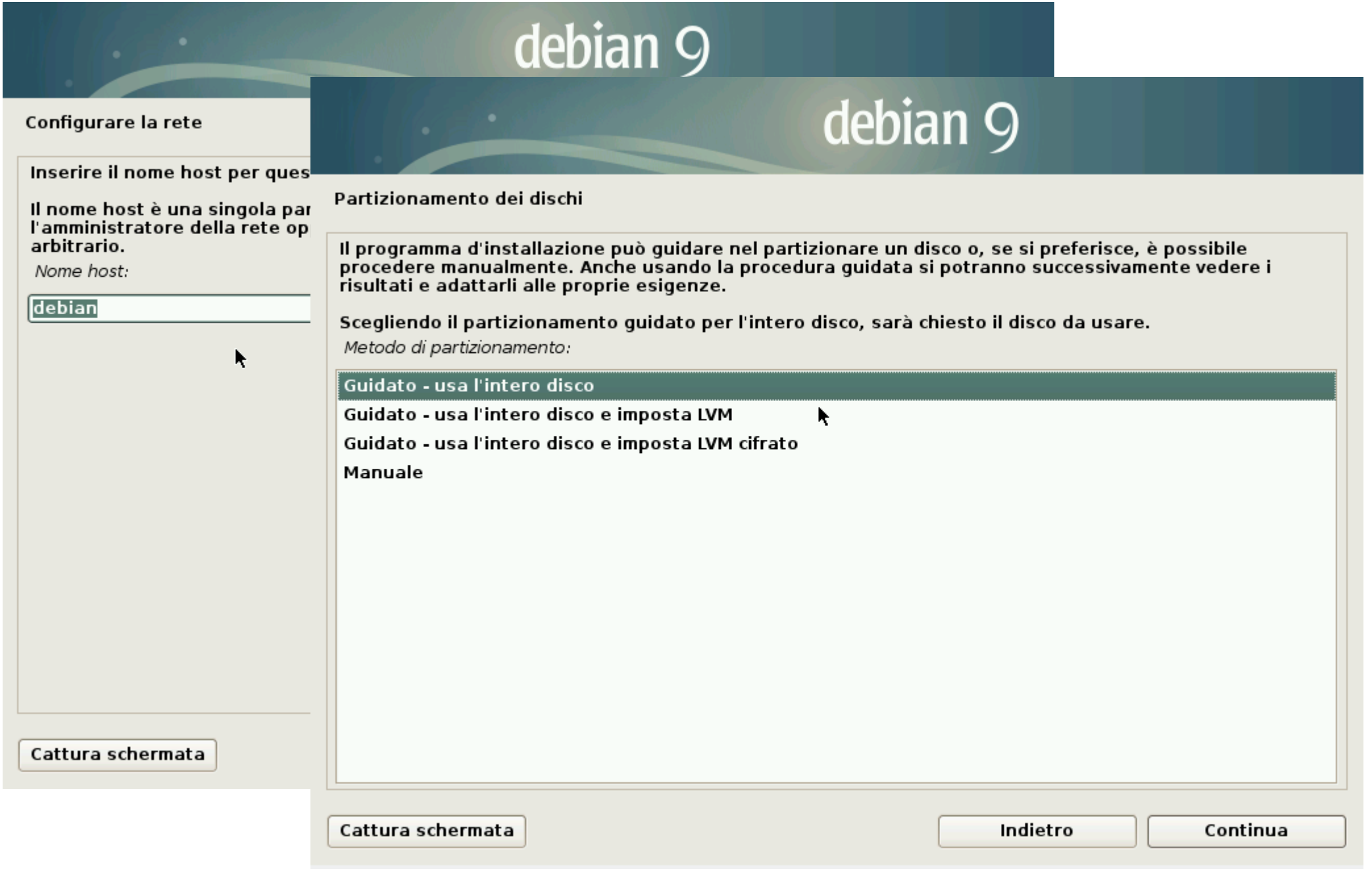

CREA UTENTE
Fatto
INSTALLAZIONE FEDORA 27
it
Aiuto!
Nome completo
fedora
User name
fedora
Suggerimento: Si consiglia di tenere un nome utente più breve di 32 caratteri e senza spazi.
Imposta questo utente come amministratore
Richiedi una password per usare questo account
Password
Debole
Conferma password
Avanzato...
La password inserita è debole: La password non supera il controllo del dizionario - Si basa su un termine di dizionario. Occorre premere due volte Fatto per

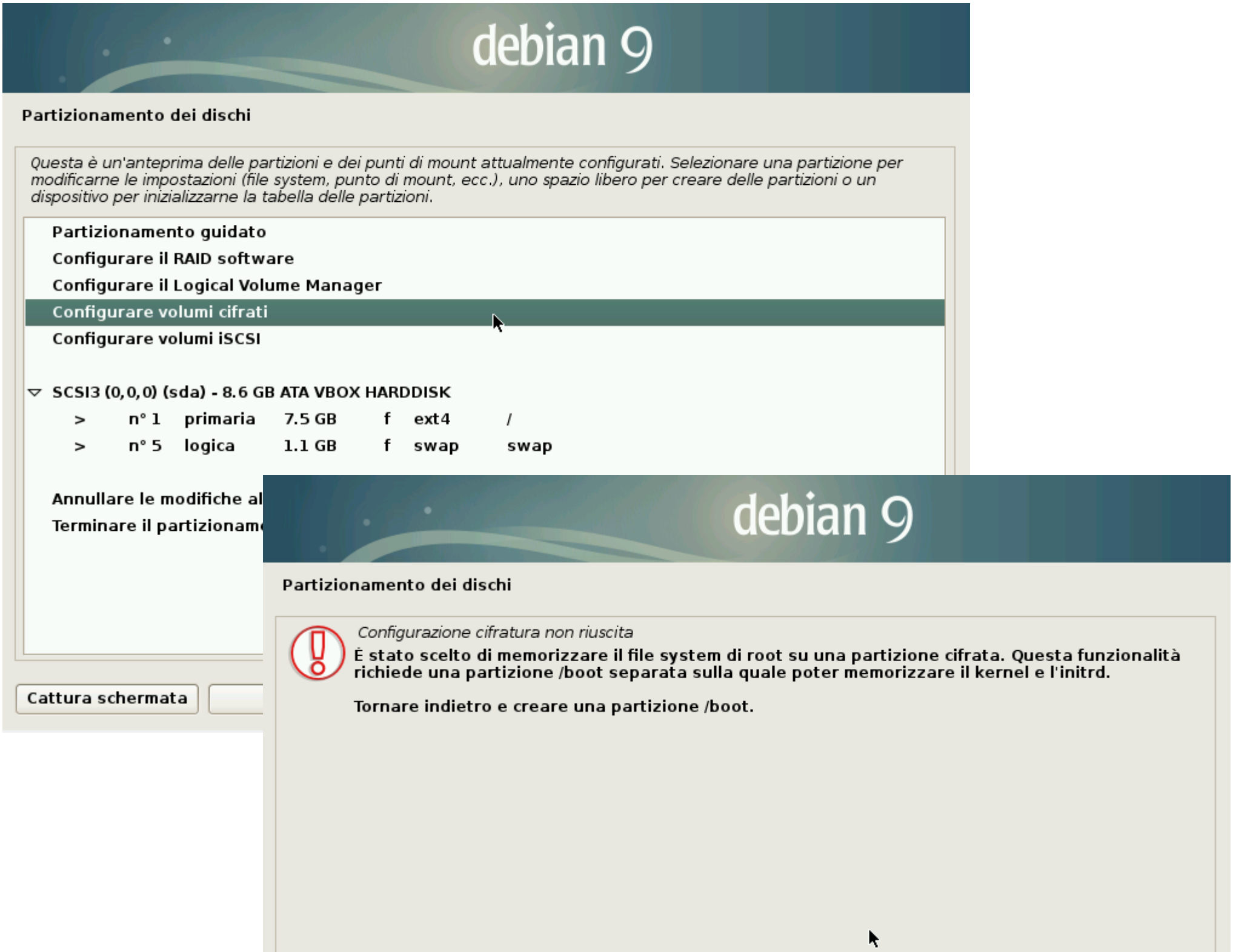

File Macchina Visualizza Inserimento Dispositivi Aiuto
Please enter passphrase for disk VBOX_HARDDISK (luks-70d3b84a-ea9f-4e44-8f29-31a4ae756944)!:*********
****
Ctrl destro

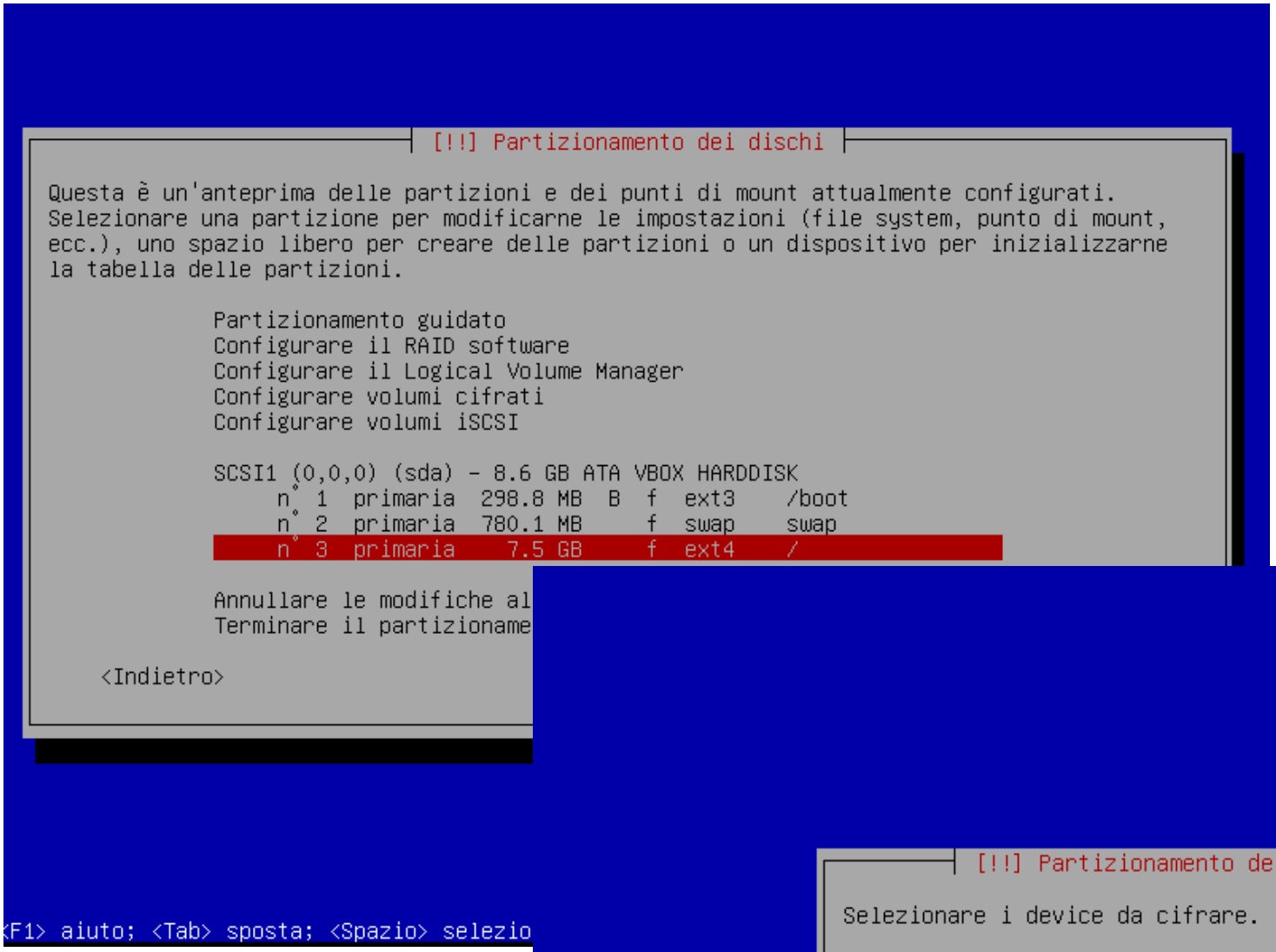

File Macchina Visualizza Inserimento Dispositivi Aiuto
Starting Cleaning Up and Shutting Down Daemons...
[OK] Stopped target Remote File Systems.
[OK] Stopped target Remote File Systems (Pre).
[OK] Stopped dracut cmdline hook.
Starting Setup Virtual Console...
Starting Plymouth switch root service...
[OK] Stopped dracut initqueue hook.
[OK] Stopped target Timers.
[OK] Stopped target Initrd Default Target.
Stopping Forward Password Requests to Plymouth...
[OK] Stopped target Basic System.
[OK] Stopped target System Initialization.
[OK] Stopped target Local Encrypted Volumes.
[OK] Stopped target Swap.
[OK] Stopped Apply Kernel Variables.
Stopping udev Kernel D
[OK] Stopped udev Coldplug
[OK] Stopped Create Volatil
[OK] Stopped target Local F
[OK] Stopped target Sockets
[OK] Stopped target Slices.
[OK] Stopped target Initrd
[OK] Stopped target Paths.
[OK] Stopped udev Kernel De
[OK] Stopped Forward Passwo
[OK] Started Cleaning Up an
[OK] Stopped Create Static
[OK] Stopped Create list of
[OK] Closed udev Kernel Soc
[OK] Closed udev Control So
Starting Cleanup udevd
[OK] Started Plymouth switc
[OK] Started Cleanup udevd
[OK] Started Setup Virtual
[OK] Reached target Switch
Starting Switch Root..
File Macchina Visualizza Inserimento Dispositivi Aiuto
Fedora 27 (Twenty Seven)
Kernel 4.13.13-300.fc27.x86_64 on an x86_64 (tty1)
Hint: Num Lock on
localhost login: _

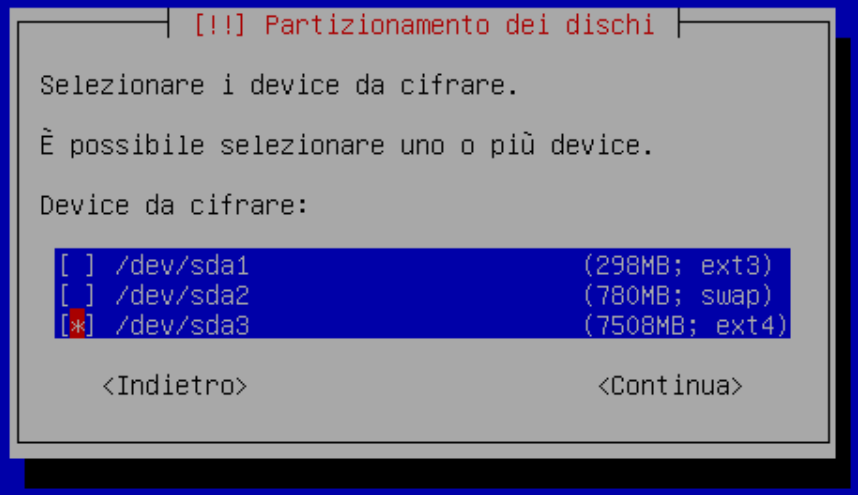
Encrypted Filesystem

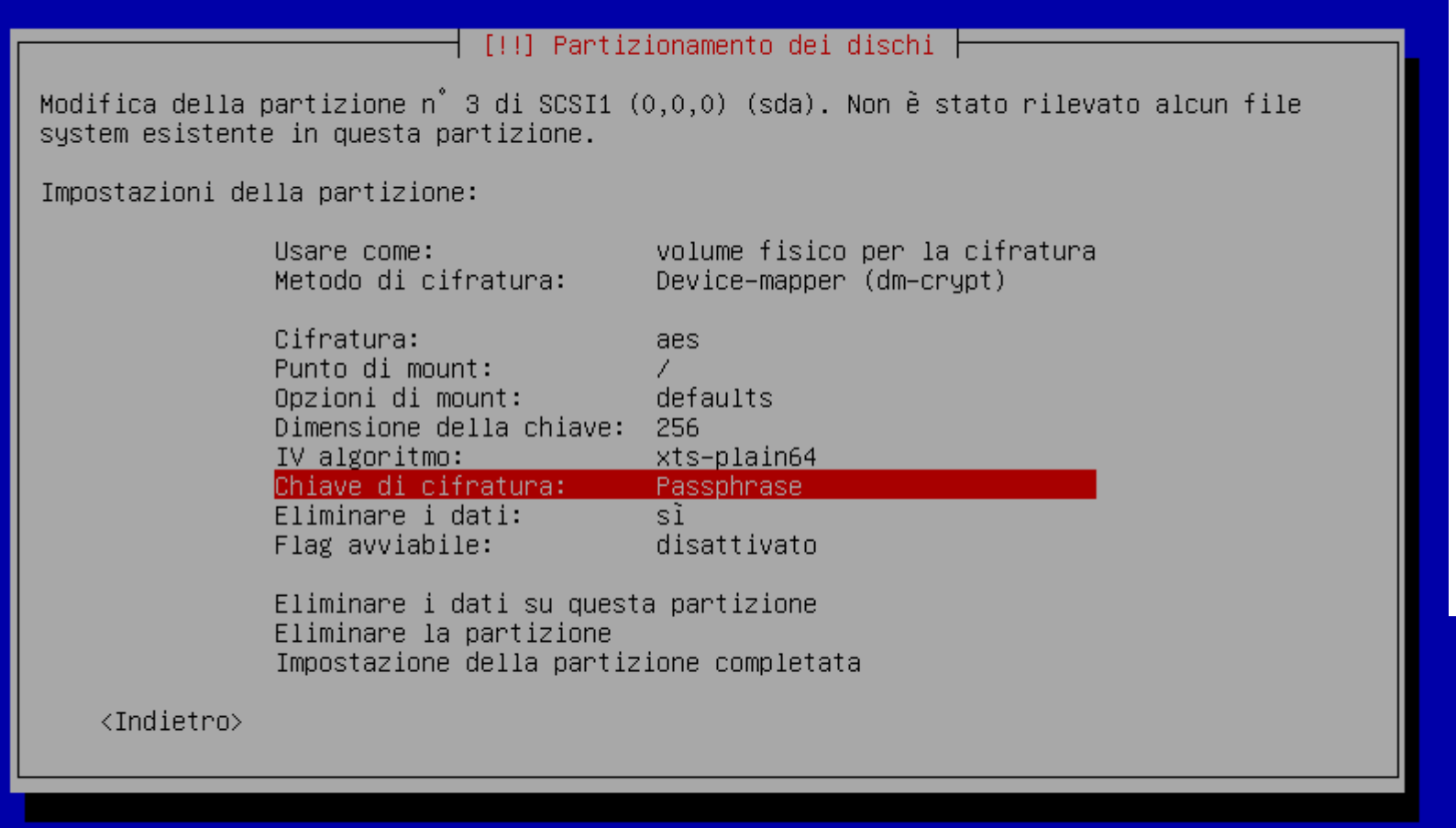
(installazione Debian style)




debian 9
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) - 8.6 GB ATA VBOX HARDDISK
> n° 1 primaria 7.5 GB f ext4 /
> n° 5 logica 1.1 GB f swap swap
Annullare le modifiche al
Terminare il partizionam
Cattura schermata
debian 9
Partizionamento dei dischi
Configurazione cifratura non riuscita
È stato scelto di memorizzare il file system di root su una partizione cifrata. Questa funzionalità richiede una partizione /boot separata sulla quale poter memorizzare il kernel e l'initrd.
Tornare indietro e creare una partizione /boot.


[!!] 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
SCSI1 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK
n° 1 primaria 298.8 MB B f ext3 /boot
n° 2 primaria 780.1 MB f swap swap
n° 3 primaria 7.5 GB f ext4 /
Annullare le modifiche al
Terminare il partizioname
<Indietro>
<F1> aiuto; <Tab> sposta; <Spazio> selezio

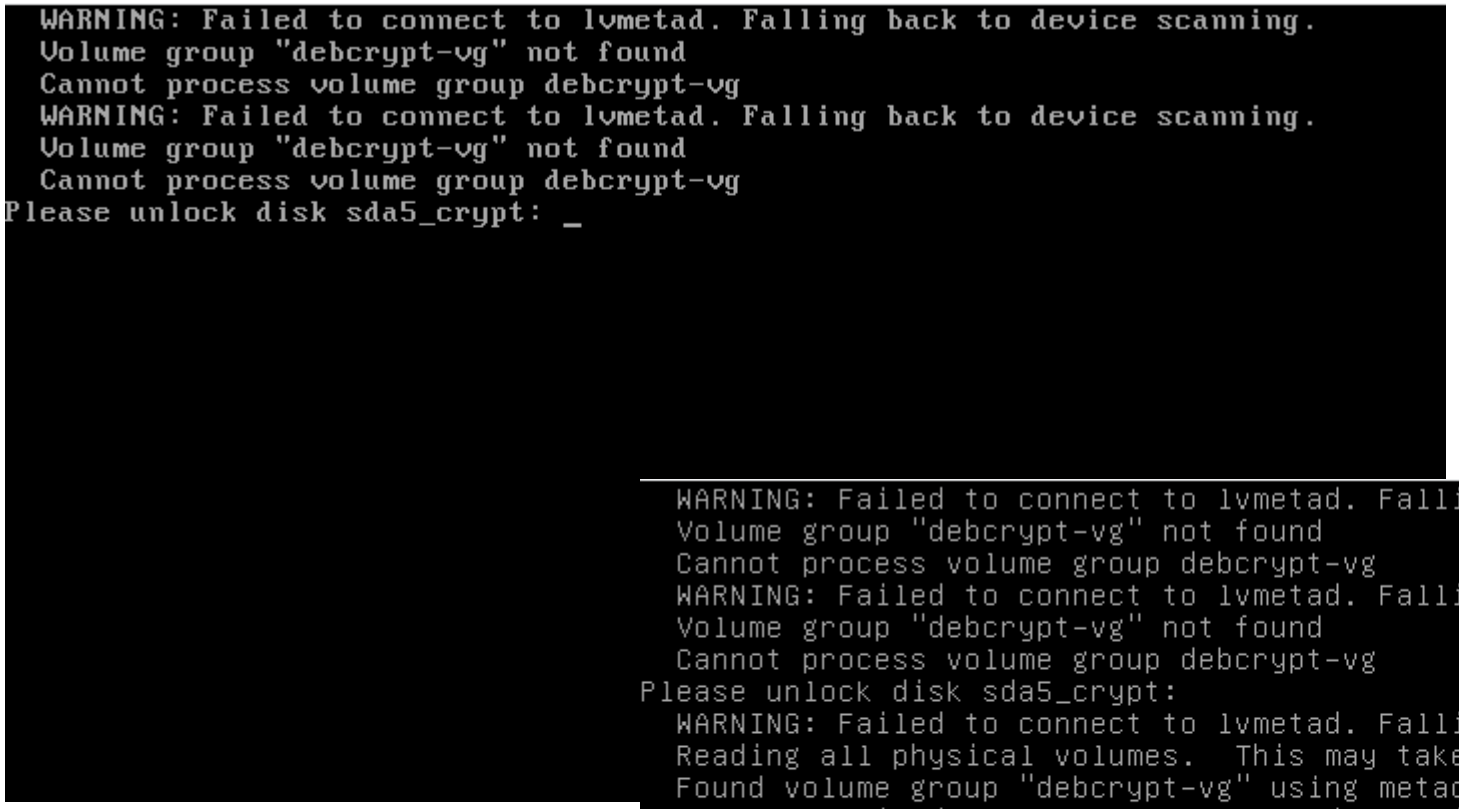

[!!] Partizionamento dei dischi
Selezionare i device da cifrare.
È possibile selezionare uno o più device.
Device da cifrare:
[ ] /dev/sda1 (298MB; ext3)
[ ] /dev/sda2 (780MB; swap)
[*] /dev/sda3 (7508MB; ext4)
<Indietro>
<Continua>

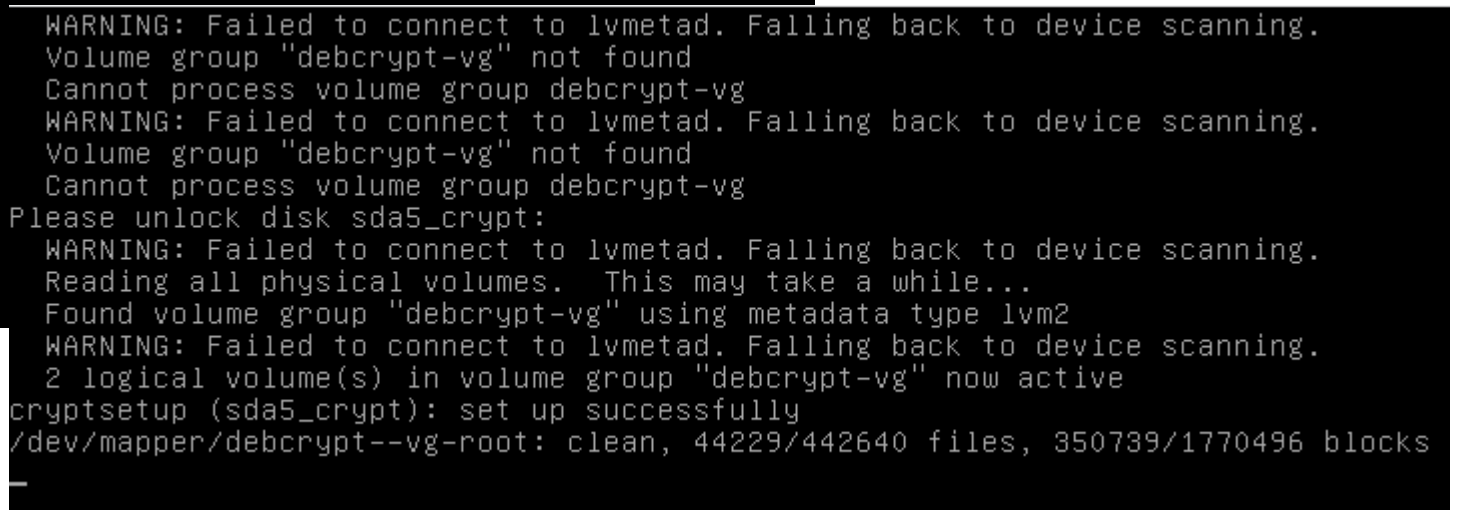

[!!] Partizionamento dei dischi
Modifica della partizione n° 3 di SCSI1 (0,0,0) (sda). Non è stato rilevato alcun file system esistente in questa partizione.
Impostazioni della partizione:
Usare come: volume fisico per la cifratura
Metodo di cifratura: Device-mapper (dm-crypt)
Cifratura: aes
Punto di mount: /
Opzioni di mount: defaults
Dimensione della chiave: 256
IV algoritmo: xts-plain64
Chiave di cifratura: Passphrase
Eliminare i dati: sì
Flag avviabile: disattivato
Eliminare i dati su questa partizione
Eliminare la partizione
Impostazione della partizione completata
<Indietro>

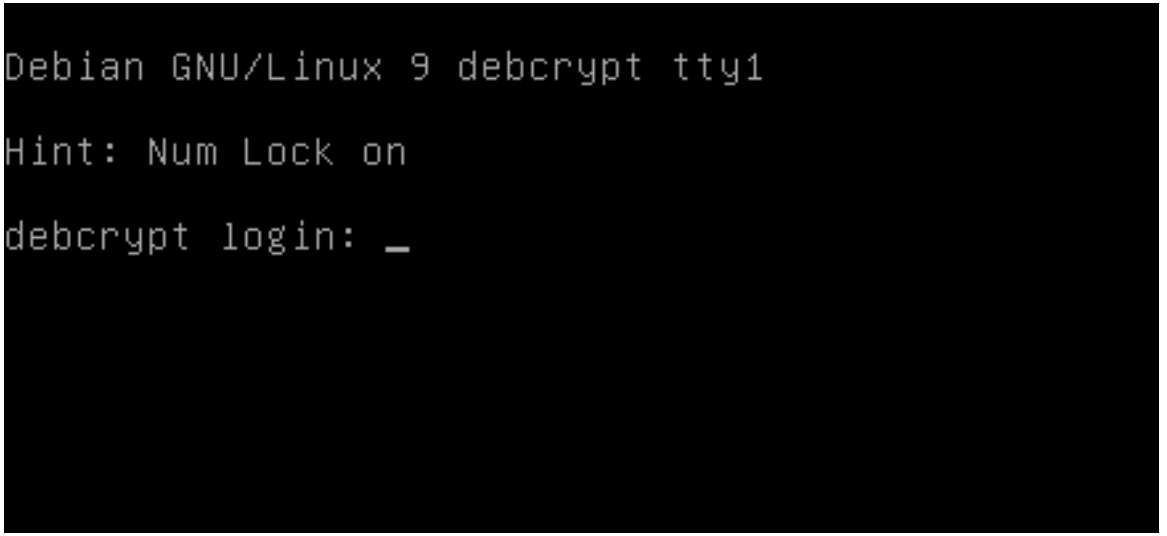
F1> aiuto; <Tab> sposta; <Spazio> seleziona; <Invio> attiva i pulsanti

[!!] Partizionamento dei dischi
Tipo di chiave di cifratura per questa partizione:
Passphrase
Chiave casuale
<Indietro>

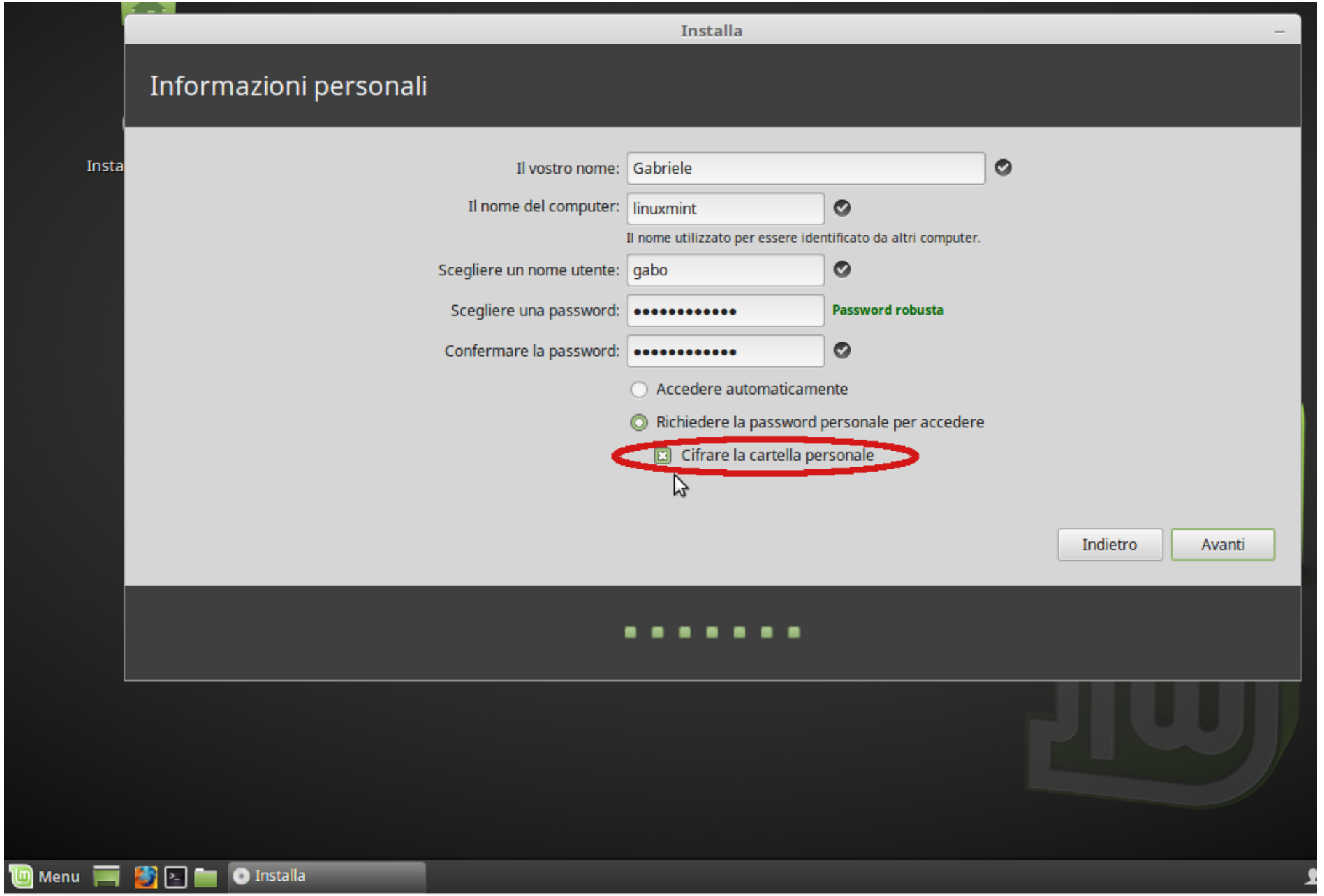

debian 9
Partizionamento dei dischi
Questa è un'anteprima delle partizioni e dei punti di mount attualmente configurati. Selezionare una partizione per modificarne le impostazioni (file system, punto di mount, ecc.), uno spazio libero per creare delle partizioni o un dispositivo per inizializzarne la tabella delle partizioni.
Configurare il Logical Volume Manager
Configurare volumi cifrati
Configurare volumi iSCSI
LVM VG debcrypt-vg, LV root - 7.3 GB Linux device-mapper (linear)
> n° 1 7.3 GB f ext4 /
LVM VG debcrypt-vg, LV swap_1 - 1.1 GB Linux device-mapper (linear)
> n° 1 1.1 GB f swap swap
Volume cifrato (sda5_crypt) - 8.3 GB Linux device-mapper (crypt)
> n° 1 8.3 GB K lvm
SCSI3 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK
> n° 1 primaria 254.8 MB F ext2 /boot
> n° 5 logica 8.3 GB K crypto (sda5_crypt)
Annullare le modifiche alle partizioni
Terminare il partizionamento e scrivere le modifiche sul disco
Cattura schermata
Aiuto
Indietro
Continua


WARNING: Failed to connect to lvmetad. Falling back to device scanning.
Volume group "debcrypt-vg" not found
Cannot process volume group debcrypt-vg
WARNING: Failed to connect to lvmetad. Falling back to device scanning.
Volume group "debcrypt-vg" not found
Cannot process volume group debcrypt-vg
Please unlock disk sda5_crypt: _


WARNING: Failed to connect to lvmetad. Falling back to device scanning.
Volume group "debcrypt-vg" not found
Cannot process volume group debcrypt-vg
WARNING: Failed to connect to lvmetad. Falling back to device scanning.
Volume group "debcrypt-vg" not found
Cannot process volume group debcrypt-vg
Please unlock disk sda5_crypt:
WARNING: Failed to connect to lvmetad. Falling back to device scanning.
Reading all physical volumes. This may take a while...
Found volume group "debcrypt-vg" using metadata type lvm2
WARNING: Failed to connect to lvmetad. Falling back to device scanning.
2 logical volume(s) in volume group "debcrypt-vg" now active
cryptsetup (sda5_crypt): set up successfully
/dev/mapper/debcrypt--vg-root: clean, 44229/442640 files, 350739/1770496 blocks
_


Debian GNU/Linux 9 debcrypt tty1
Hint: Num Lock on
debcrypt login: _

Encrypted User Home Dir



NOTE FOR DEBIAN:
https://wiki.debian.org/TransparentEncryptionForHomeFolder


Linux Mint 18.3 Sylvia linuxmint tty1
linuxmint login: root
Password:
Last login: Sat Jan 6 14:55:43 CET 2018 on tty1
Welcome to Linux Mint 18.3 Sylvia (GNU/Linux 4.10.0-38-generic x86_64)
* Documentation: https://www.linuxmint.com
root@linuxmint ~ # cd /home
root@linuxmint /home # ls -la
totale 16
drwxr-xr-x 4 root root 4096 gen 6 14:47 .
drwxr-xr-x 23 root root 4096 gen 6 14:48 ..
drwxr-xr-x 3 root root 4096 gen 6 14:47 .ecryptfs
dr-x------ 3 gabo gabo 4096 gen 6 14:49 gabo
root@linuxmint /home # ls -la gabo
totale 12
dr-x------ 3 gabo gabo 4096 gen 6 14:49 .
drwxr-xr-x 4 root root 4096 gen 6 14:47 ..
lrwxrwxrwx 1 gabo gabo 56 gen 6 14:47 Access-Your-Private-Data.desktop -> /usr/share/ecryptfs-uti
ls/ecryptfs-mount-private.desktop
drwx------ 3 gabo gabo 4096 gen 6 14:49 .cache
lrwxrwxrwx 1 gabo gabo 30 gen 6 14:47 .ecryptfs -> /home/.ecryptfs/gabo/.ecryptfs
lrwxrwxrwx 1 gabo gabo 29 gen 6 14:47 .Private -> /home/.ecryptfs/gabo/.Private
lrwxrwxrwx 1 gabo gabo 52 gen 6 14:47 README.txt -> /usr/share/ecryptfs-utils/ecryptfs-mount-priv
ate.txt
root@linuxmint /home # _
Prima dell'accesso
utente Gabo


Home
File Modifica Visualizza Vai Segnalibri Aiuto
gabo
Computer
Home
Desktop
Docume...
Musica
Immagini
Video
Scaricati
File syst...
Cestino
Rete
Rete
Documenti
Immagini
Modelli
Musica
Pubblici
Scaricati
Scrivania
Video
Appunti_segreti.txt
Selezionato "Appunti_segreti.txt" (315
Appunti_segreti.txt (~)
File Modifica Visualizza Cerca Strumenti Documenti Aiuto
Caro diario,
The first release in the upcoming Linux Mint 19.x series will be named "Tara". Tara is a popular name here in Ireland, and the name of someone we really like ☺ The development cycle only just started so it's a bit early to give details about Linux Mint 19, but here's what we can say
Testo semplice
Larghezza tabulazione: 4
Rg 3, Col 288
INS
Accesso sessione utente: Gabo
Menu
Home
Appunti_segreti.txt (~)
14.59

```
root@linuxmint /home # ls -la gabo
totale 196
drwx------ 17 gabo gabo 4096 gen  6 15:06 .
drwxr-xr-x  4 root root 4096 gen  6 14:47 ..
-rw-rw-r--  1 gabo gabo  315 gen  6 14:59 Appunti_segreti.txt
-rw-------  1 gabo gabo   46 gen  6 14:55 .bash_history
-rw-r--r--  1 gabo gabo  220 gen  6 14:47 .bash_logout
-rw-r--r--  1 gabo gabo 4000 gen  6 14:47 .bashrc
drwxr-xr-x  8 gabo gabo 4096 gen  6 14:58 .cache
drwxrwxr-x  3 gabo gabo 4096 gen  6 15:06 .cinnamon
drwxr-xr-x 13 gabo gabo 4096 gen  6 15:00 .config
drwx------  3 gabo gabo 4096 gen  6 14:54 .dbus
drwxr-xr-x  2 gabo gabo 4096 gen  6 14:54 Documenti
lrwxrwxrwx  1 gabo gabo   30 gen  6 14:47 .ecryptfs -> /home/.ecryptfs/gabo/.ecryptfs
drwx------  2 gabo gabo 4096 gen  6 14:54 .gconf
-rw-------  1 gabo gabo  660 gen  6 15:06 .ICEauthority
drwxr-xr-x  2 gabo gabo 4096 gen  6 14:54 Immagini
drwxr-xr-x  3 gabo gabo 4096 gen  6 14:54 .local
drwxr-xr-x  2 gabo gabo 4096 gen  6 14:54 Modelli
drwxr-xr-x  5 gabo gabo 4096 gen  6 14:58 .mozilla
drwxr-xr-x  2 gabo gabo 4096 gen  6 14:54 Musica
lrwxrwxrwx  1 gabo gabo   29 gen  6 14:47 .Private -> /home/.ecryptfs/gabo/.Private
-rw-r--r--  1 gabo gabo  655 gen  6 14:47 .profile
drwxr-xr-x  2 gabo gabo 4096 gen  6 14:54 Pubblici
drwxr-xr-x  2 gabo gabo 4096 gen  6 14:54 Scaricati
drwxr-xr-x  2 gabo gabo 4096 gen  6 14:54 Scrivania
-rw-r--r--  1 gabo gabo    0 gen  6 14:54 .sudo_as_admin_successful
drwxr-xr-x  2 gabo gabo 4096 gen  6 14:54 Video
-rw-------  1 gabo gabo   54 gen  6 15:06 .Xauthority
-rw-------  1 gabo gabo  954 gen  6 15:07 .xsession-errors
-rw-------  1 gabo gabo 5660 gen  6 15:00 .xsession-errors.old
root@linuxmint /home #
root@linuxmint /home #
root@linuxmint /home #
root@linuxmint /home #
root@linuxmint /home # _
```

Dopo accesso utente Gabo

Nota: In linux Mint 18.3 persiste un bug per cui per un utente che esce da una sessione GUI, risulta ancora montata la sua encryptfs nella sua home ...

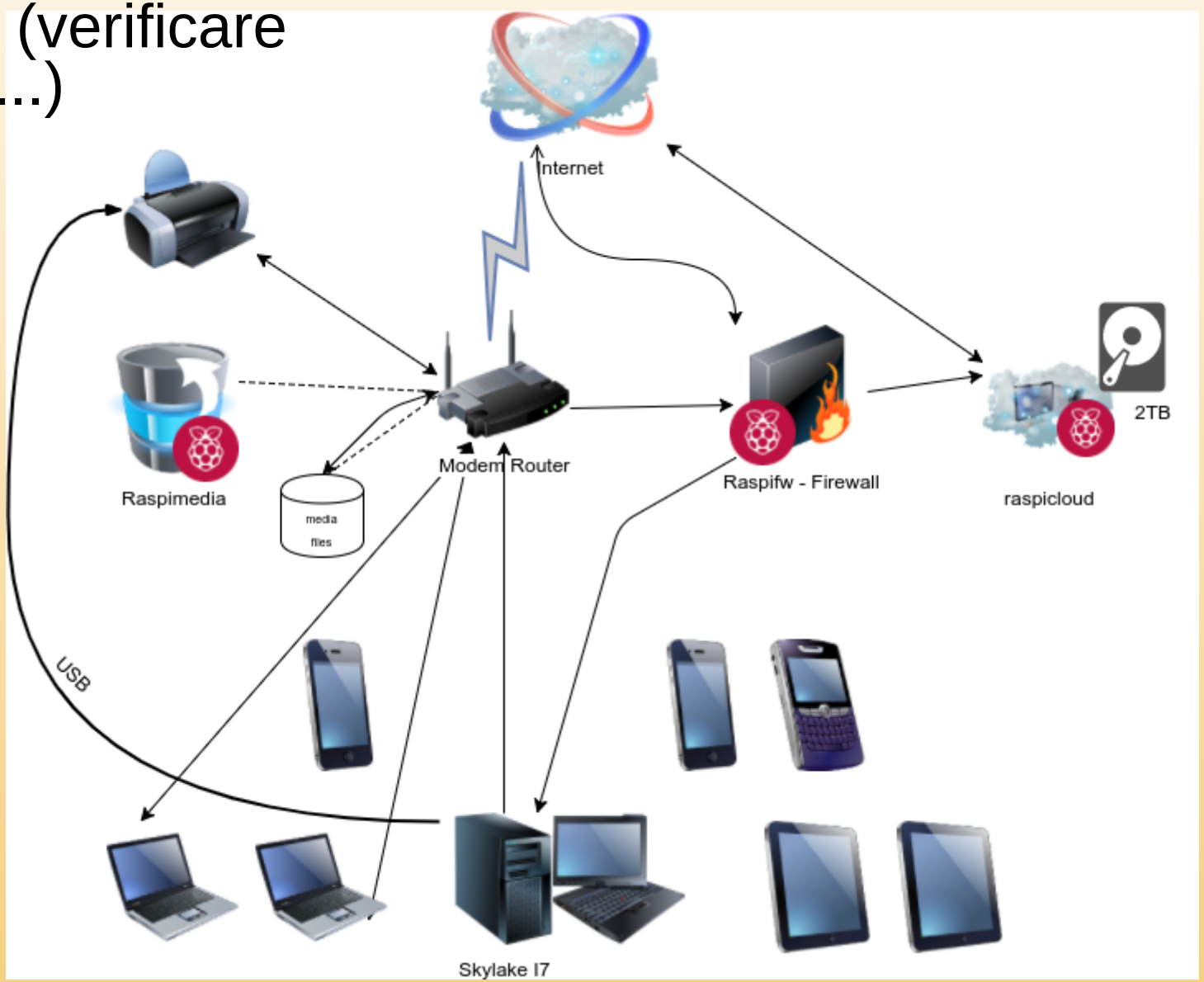
```
root@linuxmint ~ # mount | grep gabo
/home/.ecryptfs/gabo/.Private on /home/gabo type ecryptfs (rw,nosuid,nodev,relatime,ecryptfs_fnek_si
g=c0f2a82f859b4adf,ecryptfs_sig=16aec83d33acb369,ecryptfs_cipher=aes,ecryptfs_key_bytes=16,ecryptfs_
unlink_sigs)
root@linuxmint ~ # cd /home/gabo
root@linuxmint /home/gabo # ls
Appunti_segreti.txt  Documenti  Immagini  Modelli  Musica  Pubblici  Scaricati  Scrivania  Video
root@linuxmint /home/gabo # cat Appunti_segreti.txt
Caro diario,

    The first release in the upcoming Linux Mint 19.x series will be named “Tara”. Tara is a popular
 name here in Ireland, and the name of someone we really like ♦ The development cycle only just star
ted so it’s a bit early to give details about Linux Mint 19, but here’s what we can say
root@linuxmint /home/gabo #
```

Meccanismi di protezione suggeriti:

Target PC. / Metodo	PC Desktop / interactive user	PC always ON / Service Appliance / Server
BIOS User Password / HDD	✓	✗
BIOS Administrator Password	✓	✓
GRUB Adm/User Password	✓	✗
GRUB Password w/ *unrestricted* entries	✓	✓
 Encrypted filesystem	✓	✗
Encrypted home	✓	✓

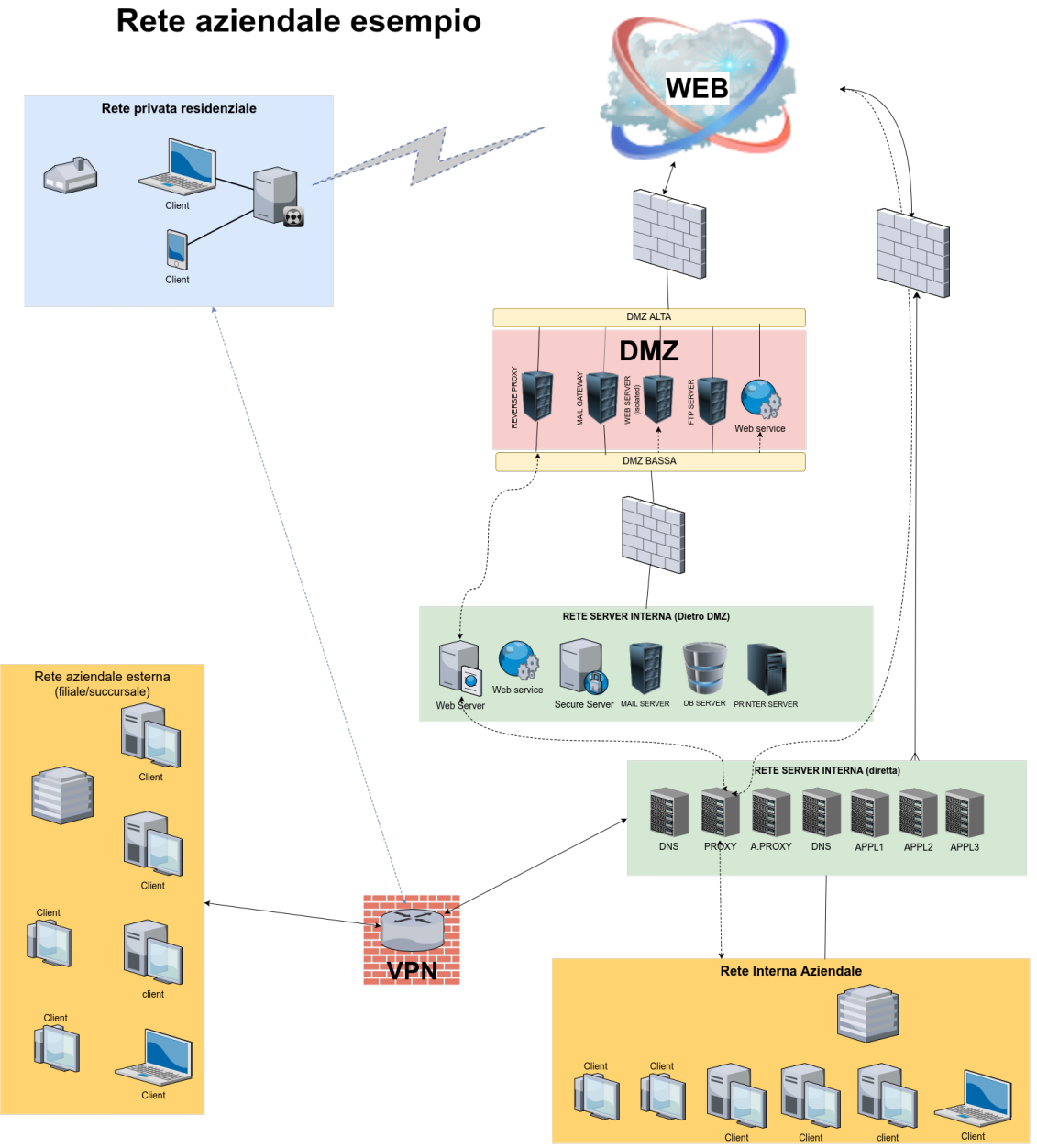
Rete uso casalingo

- Modem/Router con firewall / regole IP/Port forwarding
- DMZ del router (verificare funzionamento...)
- Collegamento piccolo appliance (rPI) come firewall



Protezione rete aziendale / medio ..

- Buona Progettazione (schema)
- RETE DMZ – Firewall/ Appliance – Rete interna



- Cenni su Selinux e Apparmor (Pro e contro di questi sistemi)

SELINUX

Usa le autorizzazioni *MAC* (Mandatory Access Control), anziché *DAC* (Discretionary Access Control).

yum install -y policycoreutils-python

Esempio per visualizzare i contesti disponibili da usare per regolare gli accessi con SELinux:

 # semanage fcontext -l

Alcuni contesti di Apache:

httpd_sys_content_t	Directory in sola lettura di apache
httpd_sys_rw_content_t	Directory in lettura scrittura di Apache. Le cartelle dove l'applicazione web può creare e modificare i file
httpd_log_t	Usato da Apache per generare/accordare i file log dell'applicazione web.
httpd_cache_t	Assegnato alla directory utilizzata da Apache per fare caching, se si utilizza mod_cache.

semanage fcontext -a -t http_sys_content_t "/webapps(/.*)?"
semanage fcontext -a -t httpd_log_t "/webapps/logs(/.*)?"
semanage fcontext -a -t httpd_cache_t "/webapps/cache(/.*)?"
**semanage fcontext -a httpd_sys_rw_content_t **
"/webapps/app1/public_html/uploads(/.*)?"
**semanage fcontext -a httpd_sys_rw_content_t **
"/webapps/app1/public_html/wp-config.php"

Per applicare le policy definite da /webapps in giù:
restorecon -Rv /webapps

Alla struttura di directory saranno applicati i seguenti contesti di SELinux:

/webapps (*httpd_sys_content_t*)
|---/apps (*httpd_sys_content_t*)
| |---/app1 (*httpd_sys_content_t*)
| |---/public_html (*httpd_sys_content_t*)
| |---/wp-content (*httpd_sys_content_t*)
| |---/uploads (*httpd_sys_rw_content_t*)
| |---....
|
|---/logs (*httpd_log_t*)
| ....
|---/cache (*httpd_cache*_t)
| ....

creative commons

Fine prima parte.
Ci rivediamo il 30 gennaio!