

Installazione con partizione Criptata LUKS con suddivisione granulare delle partizioni

Quando lavoriamo con dati dei clienti in fasi offensive o difensive e' sempre buona pratica prendere delle accortezze ulteriori per **proteggere** i loro **dati** in caso di problemi.

Un professionista **prevede e anticipa** i possibili **problem**i e complicazioni mettendo in atto misure per ridurre l'impatto o evitarli.

Criptare il disco sfruttando il **LUKS** e' una buona pratica di sicurezza.

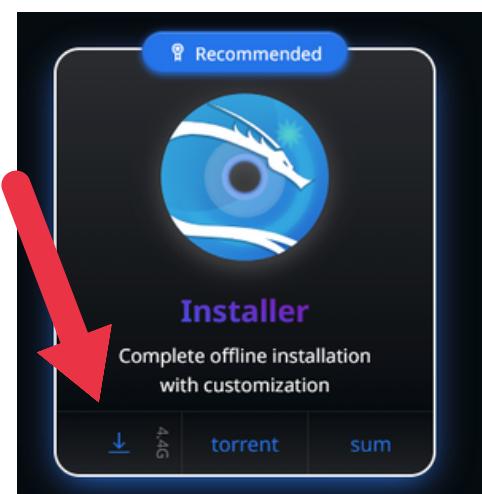
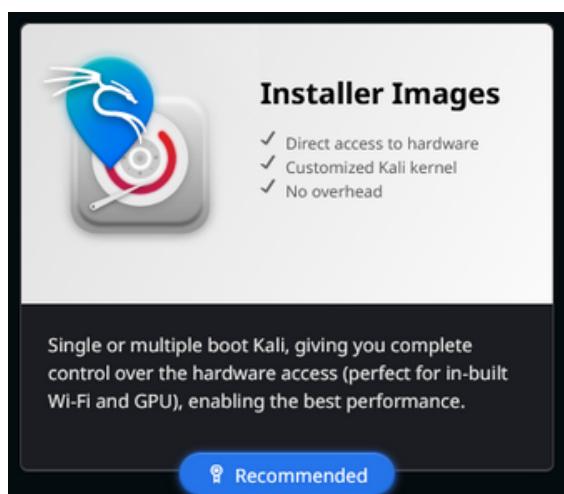
LUKS è lo **standard di sicurezza** utilizzato su Linux per **crittografare intere partizioni o dischi rigidi**, proteggendo i dati in caso di furto o smarrimento del dispositivo.

A differenza della protezione a livello di singolo file, **LUKS** opera direttamente sui blocchi del disco (**block device**), rendendo illeggibile l'intero contenuto sottostante finché non viene sbloccato. Utilizza un'intestazione (header) speciale che permette di gestire multiple password per lo stesso disco, offrendo una soluzione flessibile e indipendente dalla distribuzione utilizzata.

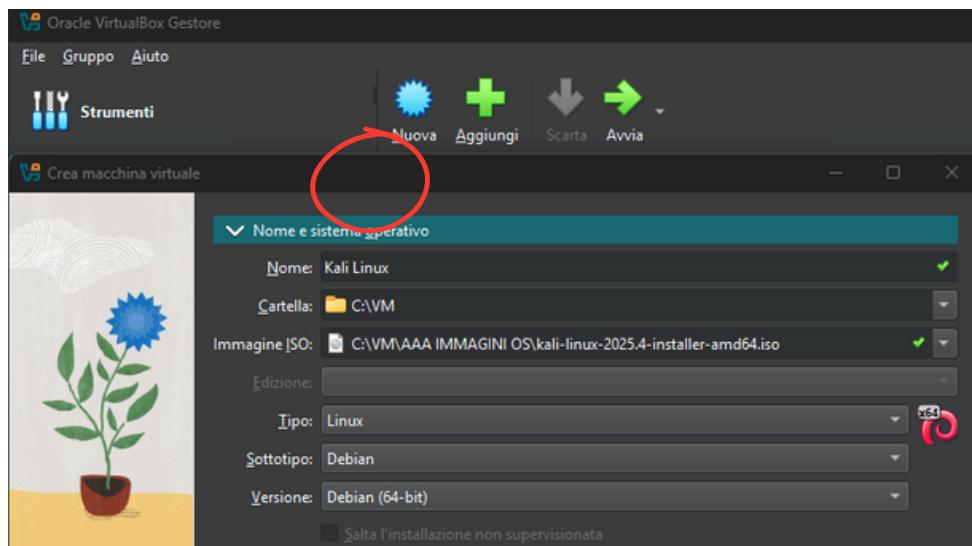
In pratica, agisce come un "**lucchetto digitale**" che **cifra** i dati prima che vengano scritti su disco e li **decifra** solo quando vengono letti **dal sistema autorizzato**

Da [Kali.org](https://kali.org) andiamo nella sezione
download e selezioniamo
Installer Images

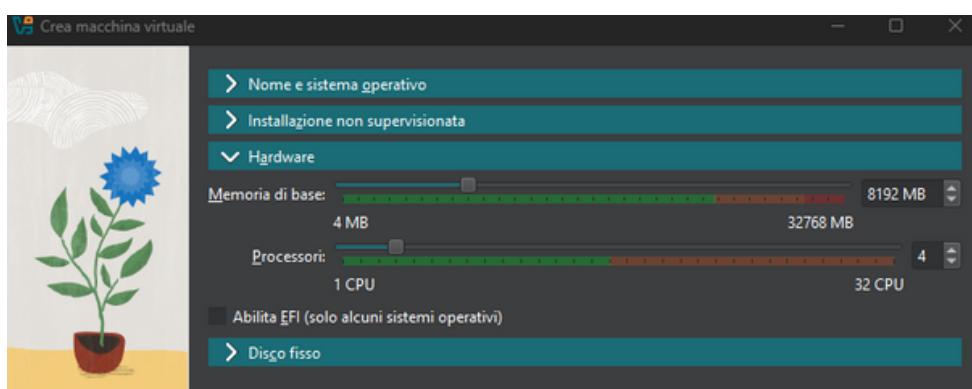
Click sul link per scaricare **ISO**



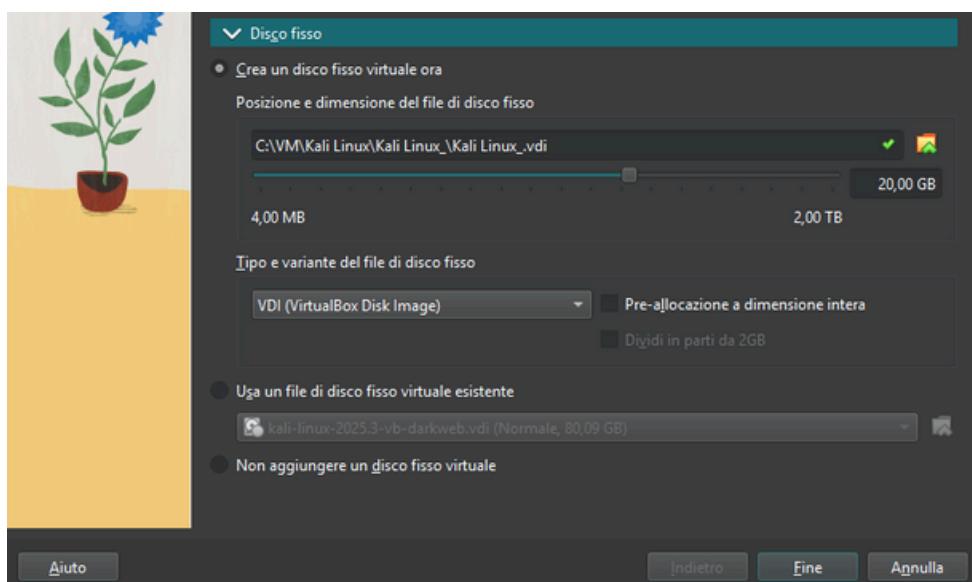
Da **Virtual Box**, selezioniamo **Nuova**
impostiamo **nome, cartella, immagine ISO, tipo, sottotipo e Versione**



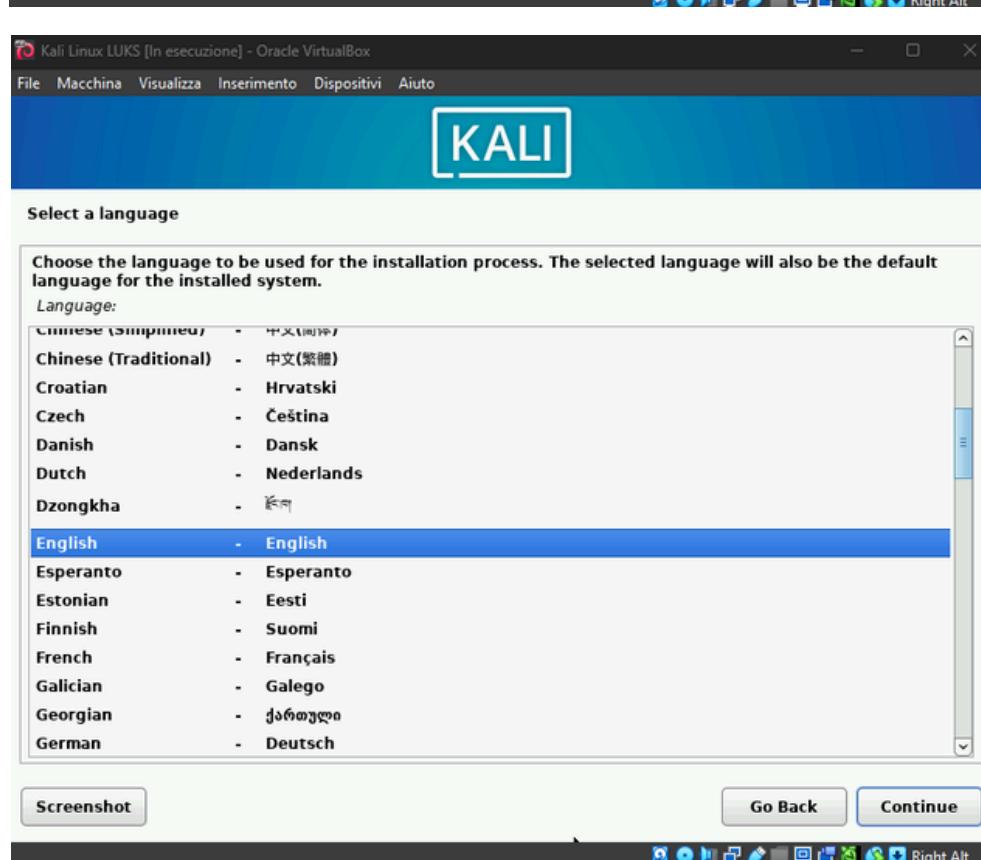
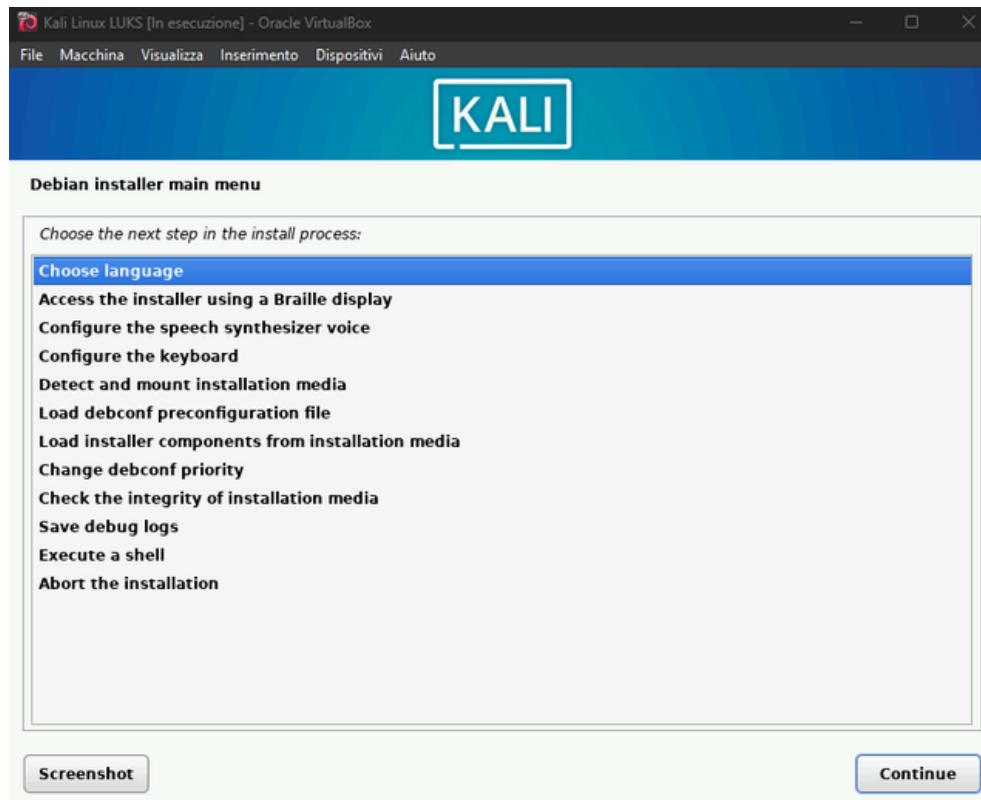
Configuriamo **la macchina virtuale** in base alle **nostre risorse**



Scegliere la **dimensione** del **harddisk** desiderato



Selezioniamo la lingua



Selezioniamo il **paese** desiderato per avere le **opzioni relative**

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

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

Country, territory or area:

- Georgia
- Germany
- Gibraltar
- Greece
- Greenland
- Guernsey
- Holy See (Vatican City State)
- Hungary
- Iceland
- Ireland
- Isle of Man
- Italy**
- Jersey

Screenshot Go Back Continue

Configure locales

There is no locale defined for the combination of language and country you have selected. You can now select your preference from the locales available for the selected language. The locale that will be used is listed in the second column.

Country to base default locale settings on:

- Hong Kong
- India
- Ireland
- Israel
- New Zealand
- Nigeria
- Philippines
- Seychelles
- Singapore
- South Africa
- United Kingdom
- United States**
- Zambia
- Zimbabwe

Screenshot Help Go Back Continue

Load installer components from installation media

Loading additional components

Retrieving nic-wireless-modules-6.16.8+kali-amd64-d1

selezioniamo la **lingua** della **tastiera**

Configure the keyboard

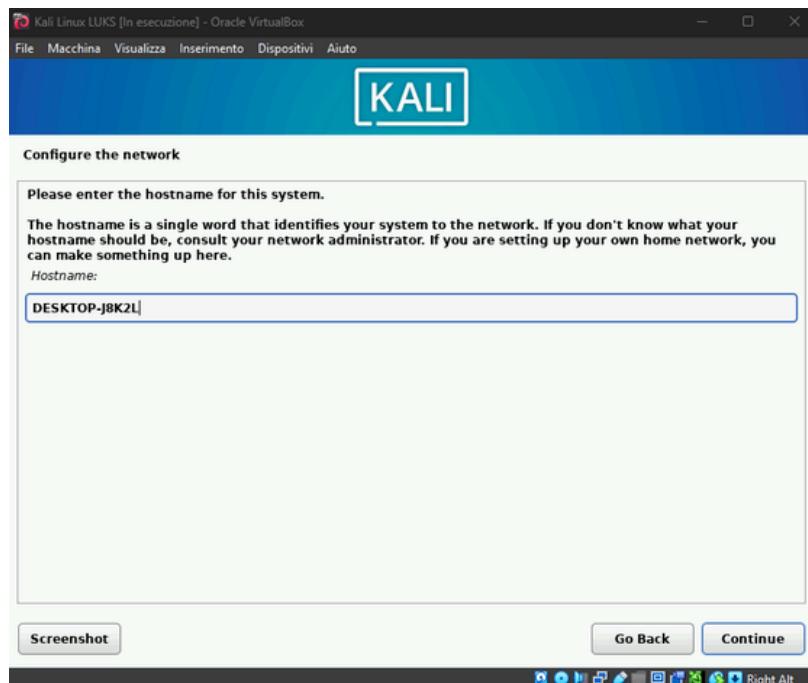
Keymap to use:

- American English**
- Albanian
- Arabic
- Asturian
- Bangladesh
- Belarusian

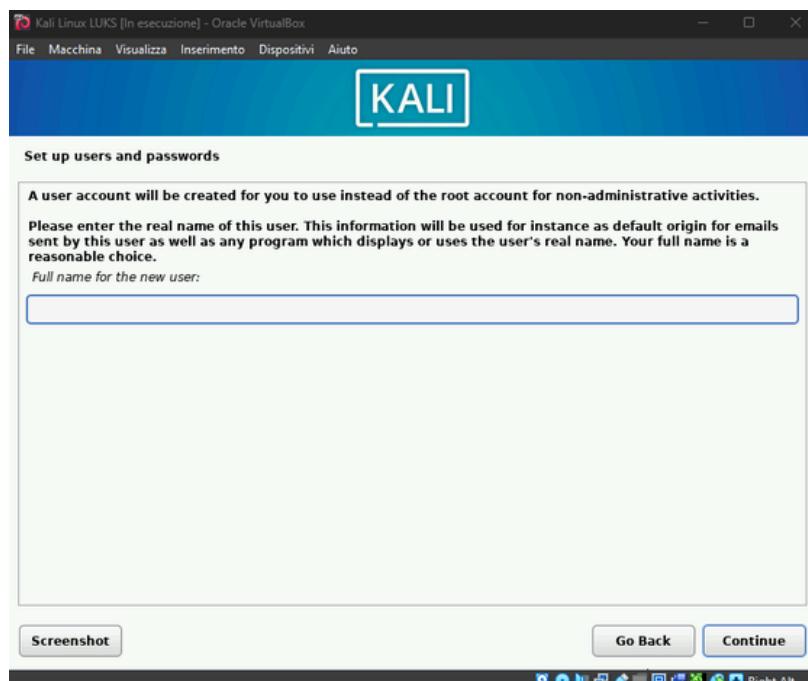
Configuriamo un hostname **generico** per dare meno nel occhio.

Esempi di nomi **HOST** di dispositivi **comuni**

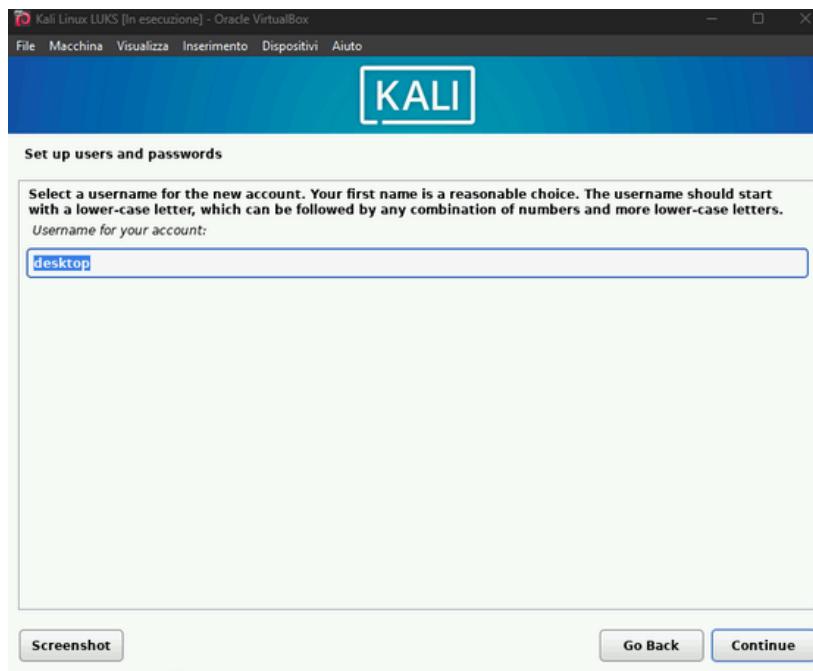
- Apple: **iPhone-di-Antonio**, **iPad-Air..**
- Windows: **DESKTOP-5A8F9**, **LAPTOP-8J2K1..**
- Altri: **Galaxy-S24**, **HPLaserJet-400**, **android-f82a9..**



Cerchiamo di rimanere coerenti nei nomi o lasciarli vuoti

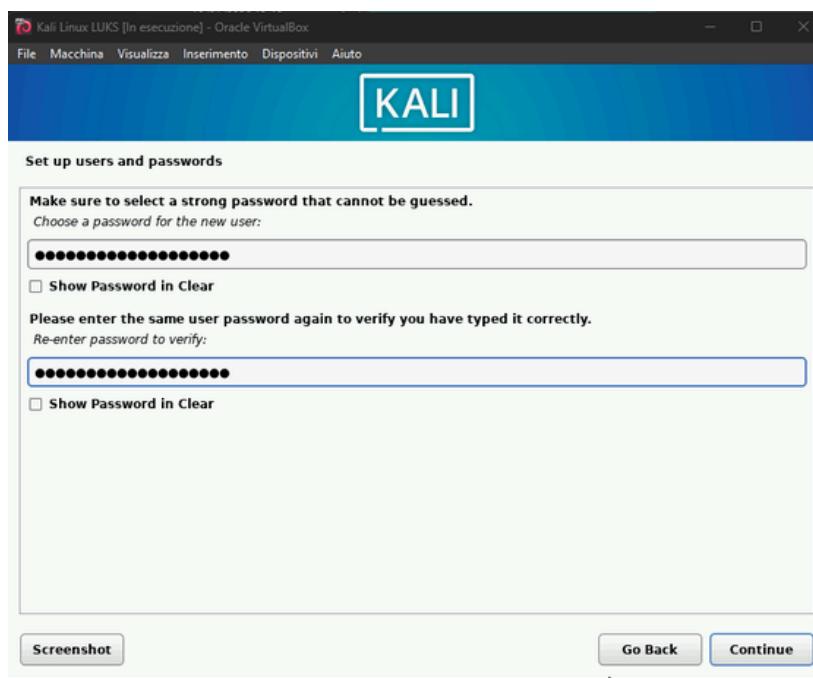


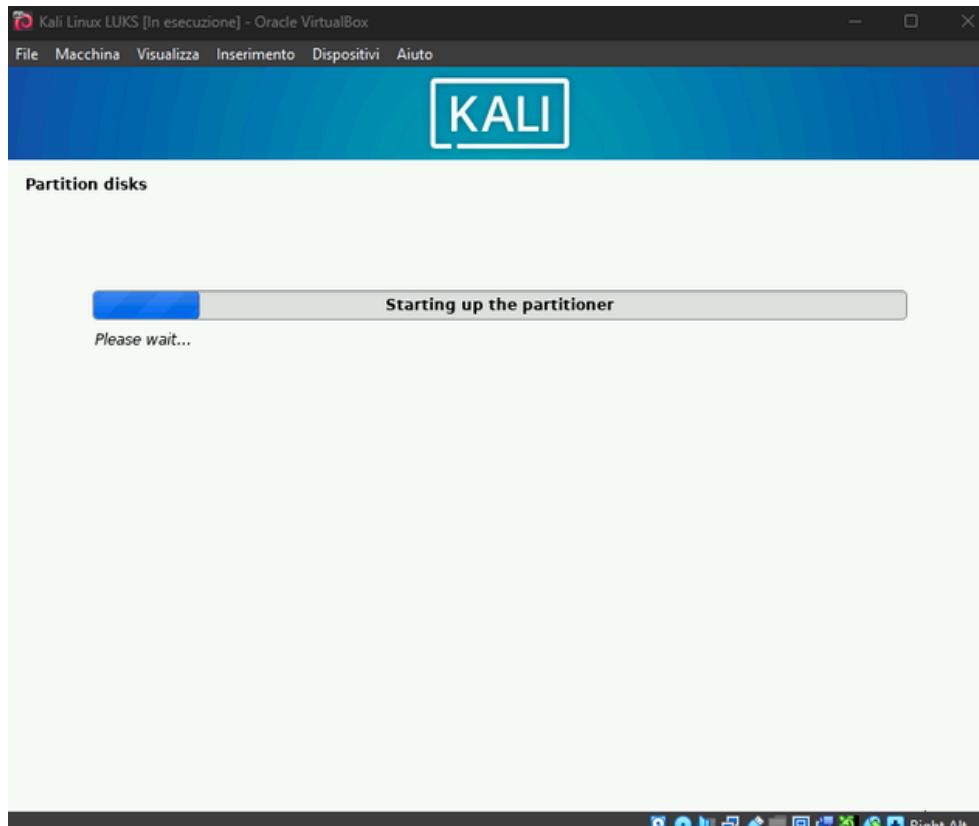
Inseriamo il **nome utente**



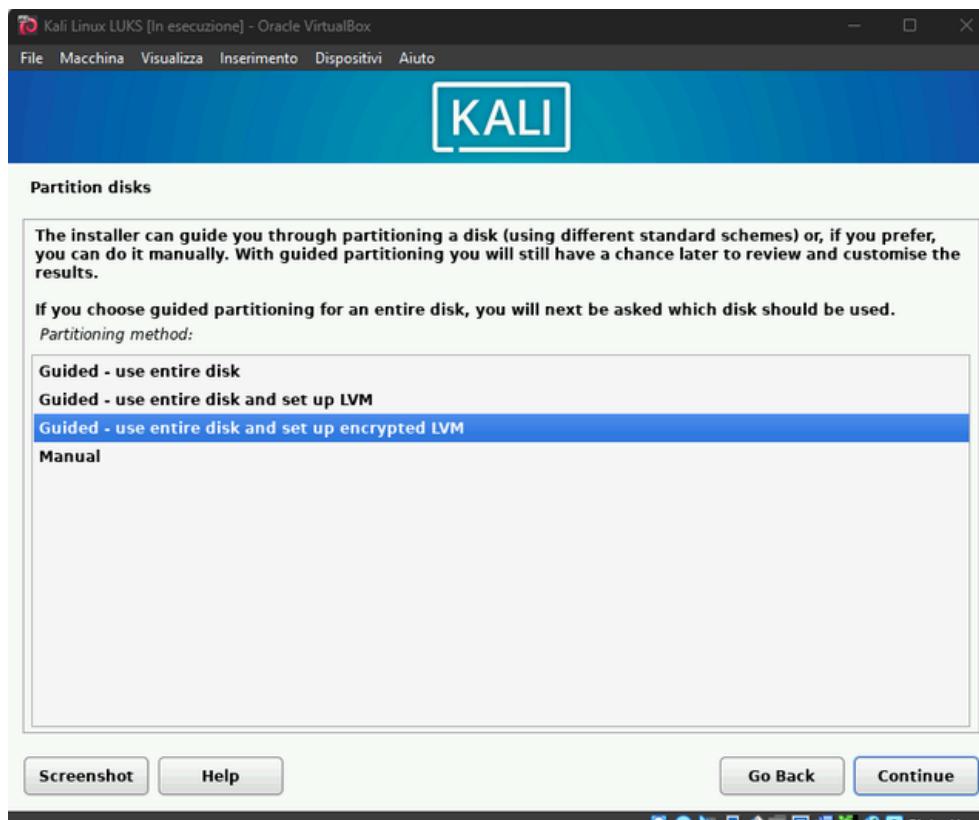
Generare una **passphrase** tra **16** e **30** caratteri.

La forza della **passphrase** e' la sua **lunghezza** e a come viene gestita

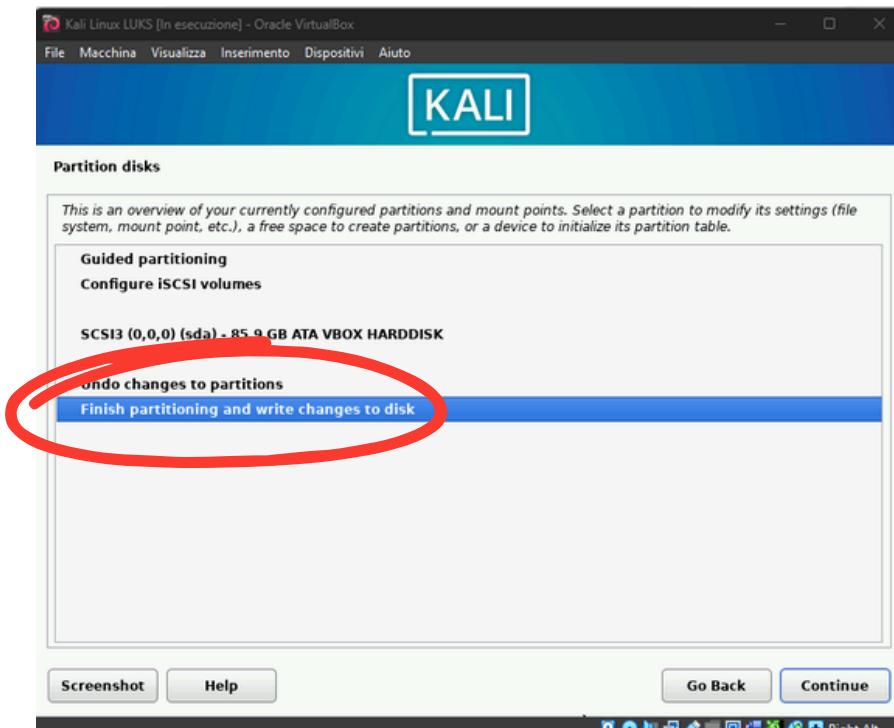




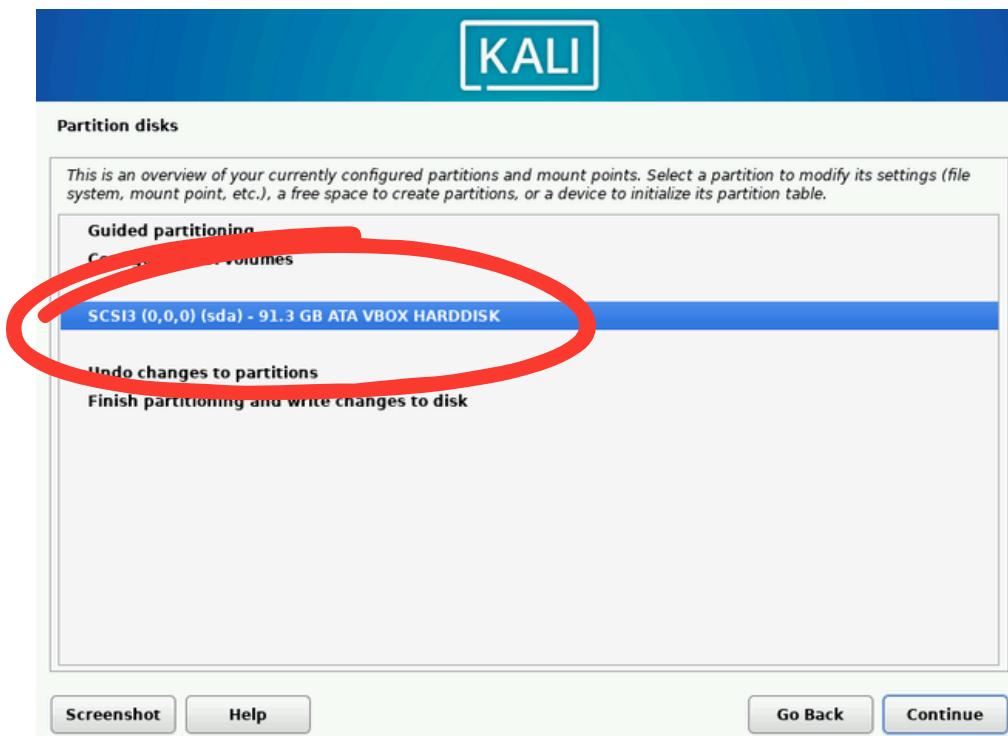
seleziona **Guided - use entire disk and set up encrypted LVM**



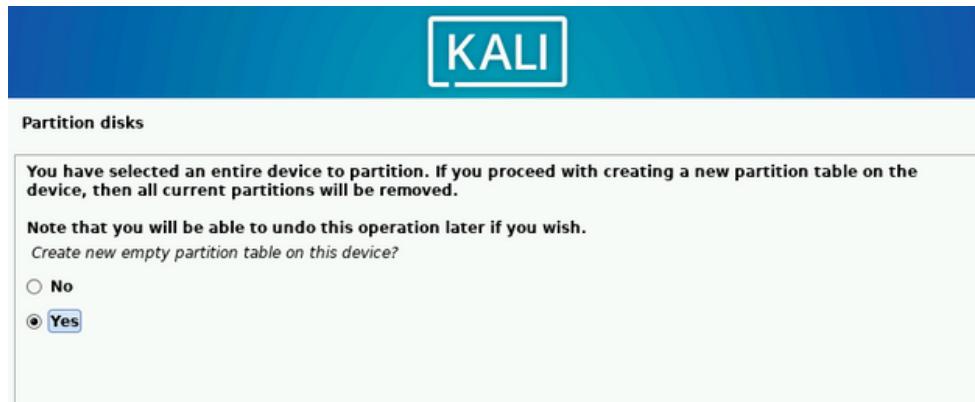
Finish partitioning and write changes to disk per lasciare il partizionamento automatico, tutto in una partizione



se vogliamo partizionare manualmente il disco selezioniamo
SCSI3 (0,0,0) - 91.3 GB ATA VBOX HARDDISK



confermiamo con YES



al termine avremo questa schermata riassuntiva della situazione

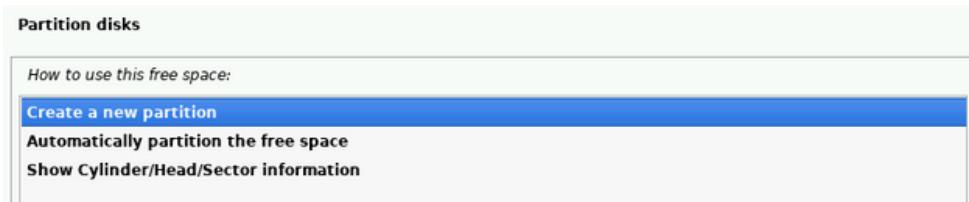


Creazione partizione di boot

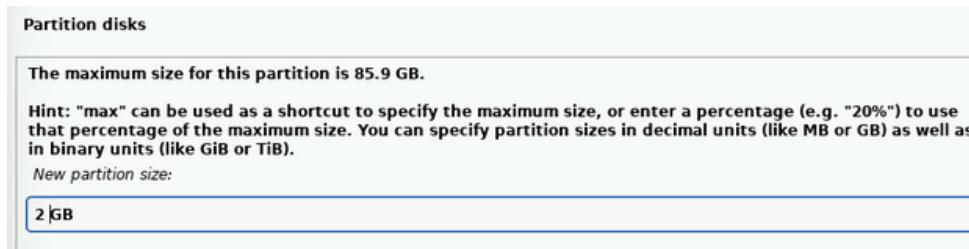
selezioniamo **FREE SPACE**



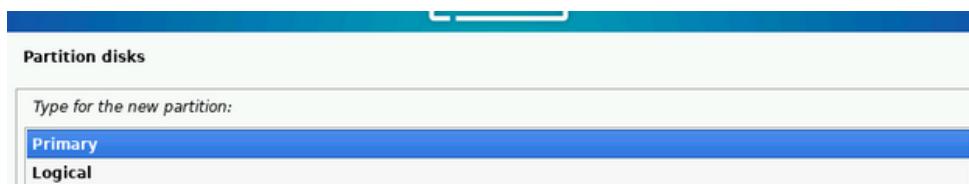
selezioniamo **Create a new partition**



selezioniamo la grandezza della partizione che useremo per il **/boot**



selezioniamo **Primary**



selezioniamo **Beginning**

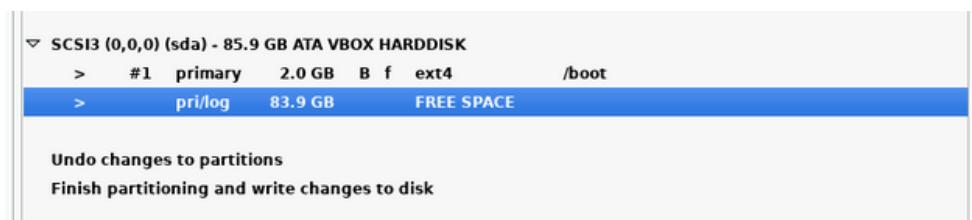


sulla voce **Mount Point**, selezioniamo **/boot**
cambiamo lo status di **Bootable flag** in **on**
e finiamo con **Done setting up the partition**

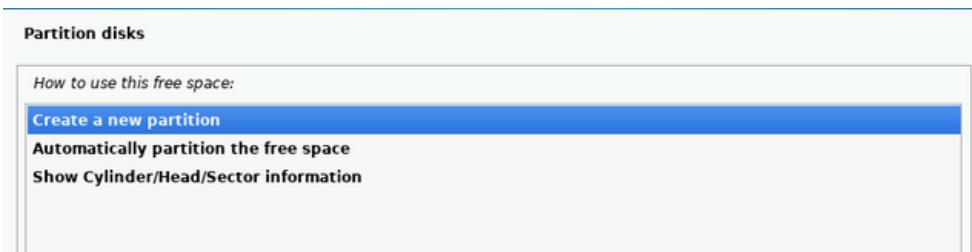


Creiamo la partizione che conterra' il volume cifrato

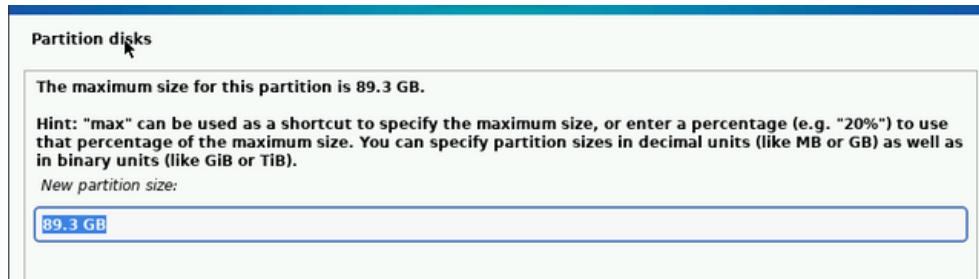
selezioniamo **FREE SPACE**



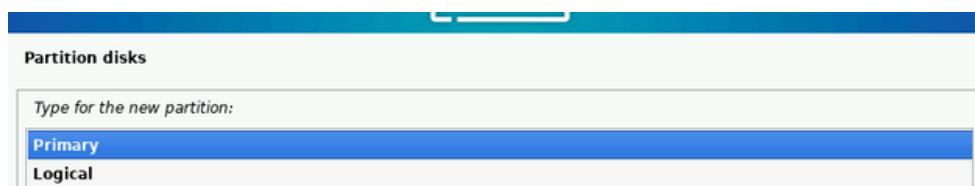
selezioniamo **Create a new partition**



selezioniamo lo **spazio rimasto** che diventerà la nostra **cassaforte cifrata**



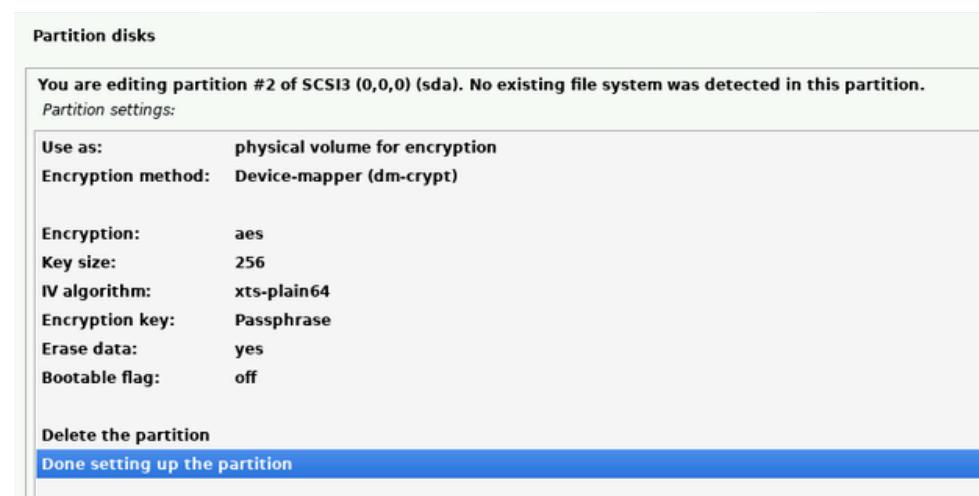
selezioniamo **Primary**



modifichiamo la voce **Use as:** in **physical volume for encryption**



selezioniamo **Done setting up the partition**



configuriamo il volume criptato

selezioniamo **Configure encrypted volumes**

Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

- Guided partitioning
- Configure software RAID
- Configure the Logical Volume Manager
- Configure encrypted volumes**
- Configure iSCSI volumes

SCSI3 (0,0,0) (sda) - 85.9 GB ATA VBOX HARDDISK

>	#1	primary	2.0 GB	B	f	ext4	/boot
>	#2	primary	83.9 GB	K	crypto		not active

selezioniamo **Yes**

Partition disks

Before encrypted volumes can be configured, the current partitioning scheme has to be written to disk. These changes cannot be undone.

After the encrypted volumes have been configured, no additional changes to the partitions on the disks containing encrypted volumes are allowed. Please decide if you are satisfied with the current partitioning scheme for these disks before continuing.

The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4

Write the changes to disk and configure encrypted volumes?

No
 Yes

selezioniamo **Create encrypted volumes**

Partition disks

This menu allows you to configure encrypted volumes.

Encryption configuration actions

- Create encrypted volumes**
- Finish

selezioniamo **/dev/sda2 (83898MB; crypto)**

Partition disks

Please select the devices to be encrypted.

You can select one or more devices.

Devices to encrypt:

<input type="checkbox"/> /dev/sda1	(1998MB; ext4)
<input checked="" type="checkbox"/> /dev/sda2	(83898MB; crypto)

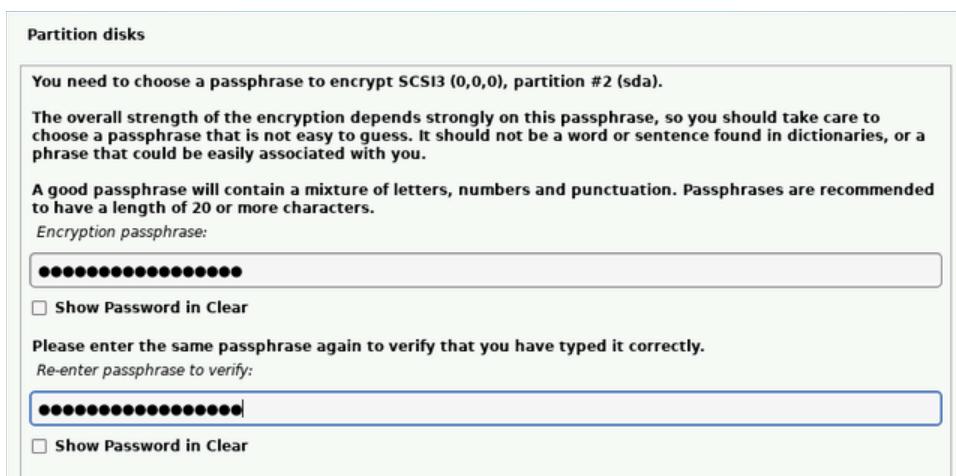
selezioniamo **Yes** e poi **Finish**



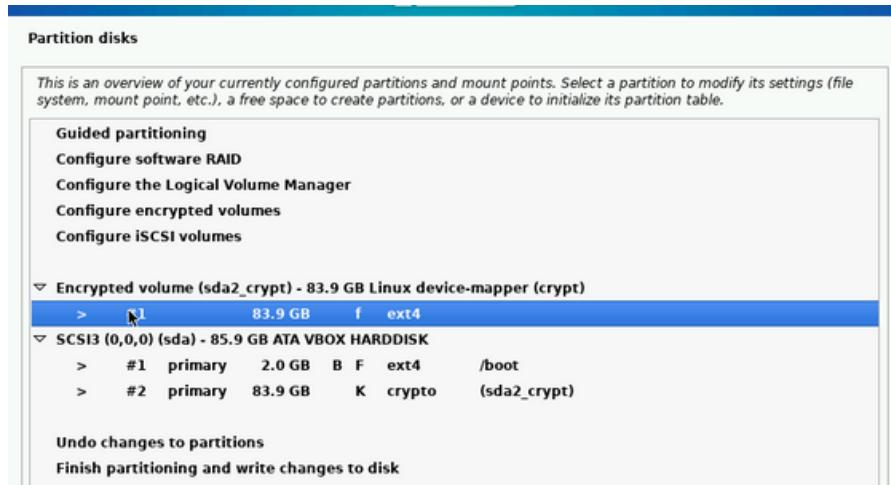
Attendiamo il completamento. Prima di inizializzare il volume cifrato, l'installer sovrascrive l'intero disco con dati casuali (misura anti-forense).



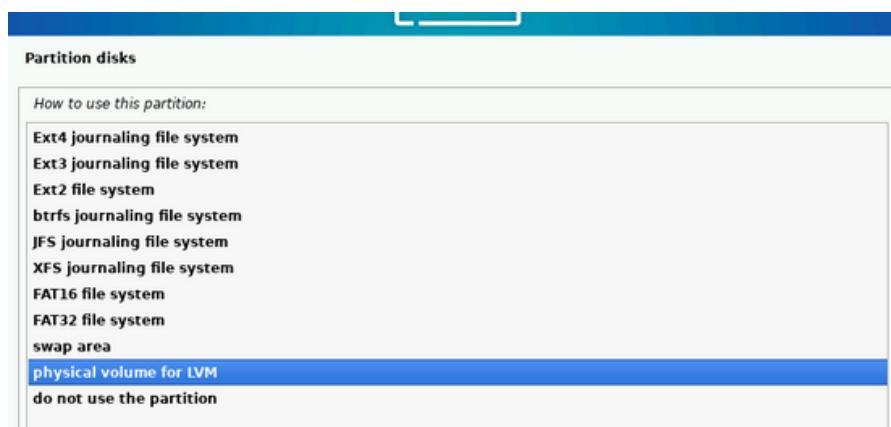
inserire la **passphrase** che **sbloccherà** il **disco rigido** all'accensione



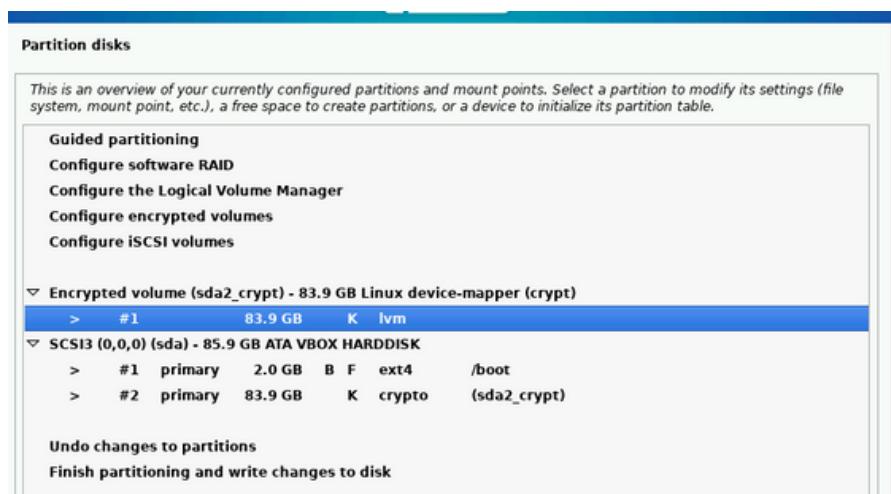
selezioniamo il volume **sda2_crypt** per *cambiarlo in volume fisico*



selezioniamo **physical volume for LVM**

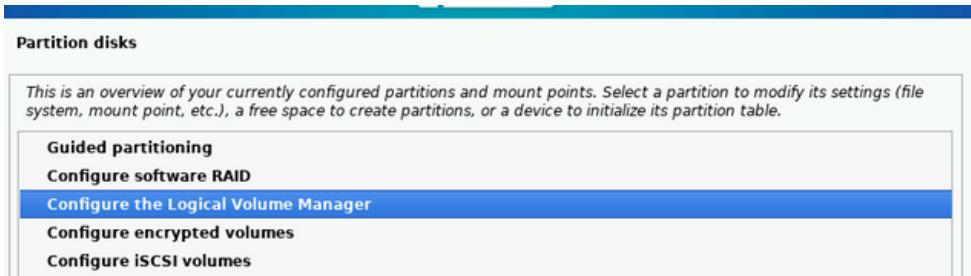


selezioniamo **sda2_crypt** ora **LVM**

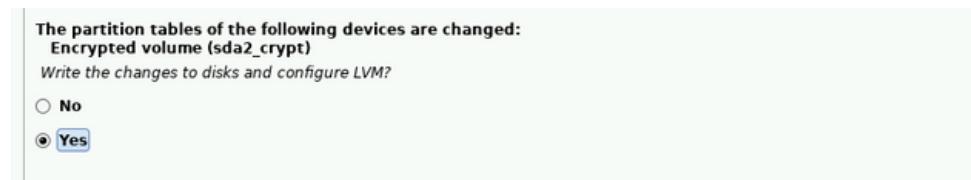


configuriamo il volume logico

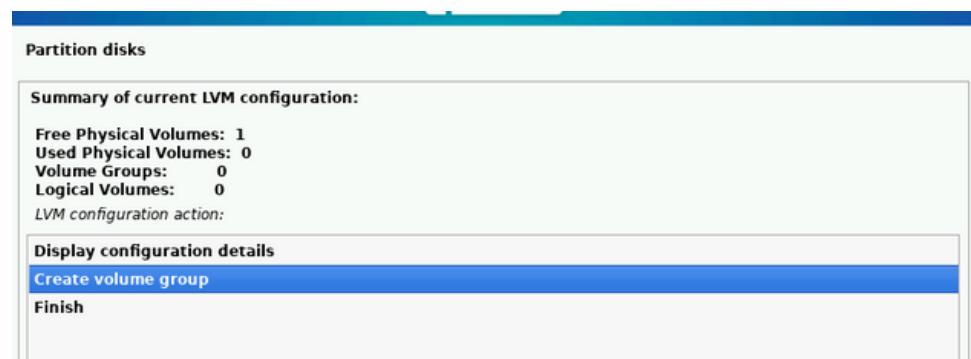
selezioniamo **Configure the Logical Volume Manager**



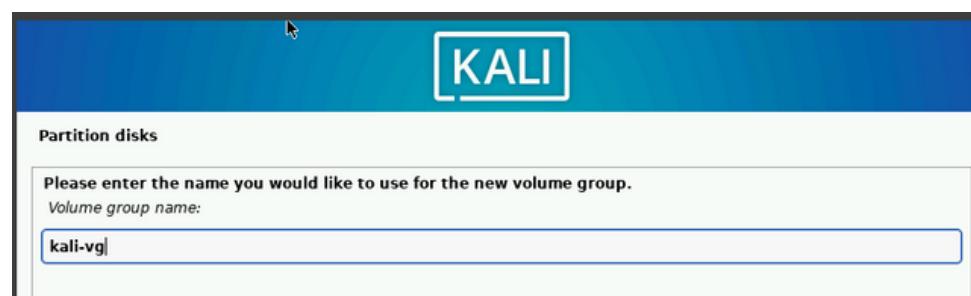
confermiamo con **Yes**



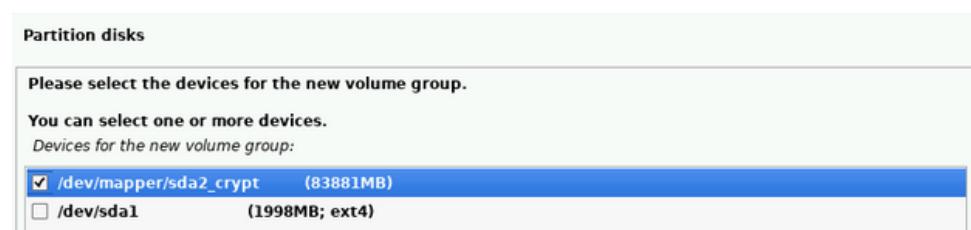
selezioniamo **Create volume group**



inserire il **nome del volume**, in questo esempio **kali-vg**



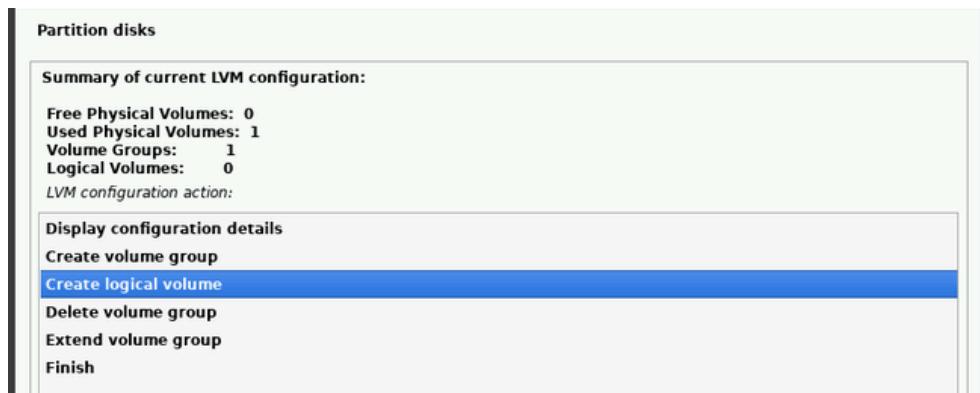
selezioniamo **/dev/mapper/sda2_crypt** (83881MB)



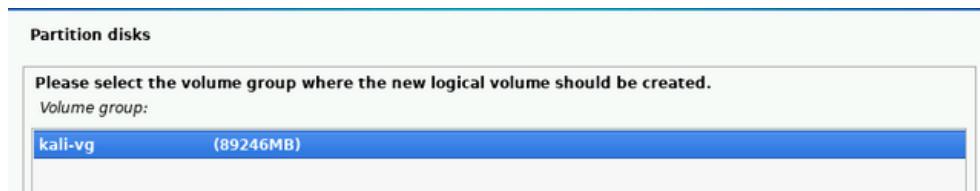
Una volta creato il **Volume Group** andiamo a creare i **Volumi Logici**.

Creazione del volume logico swap

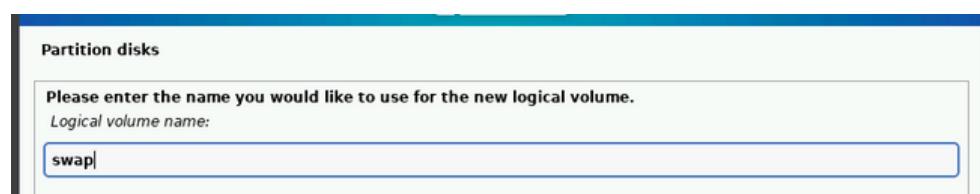
selezioniamo **Create logical volume**



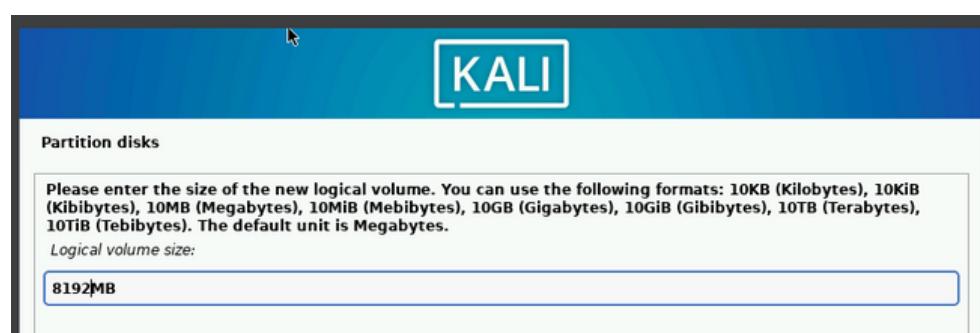
selezioniamo il **Volume Group**



inseriamo il nome del volume logico, **swap**

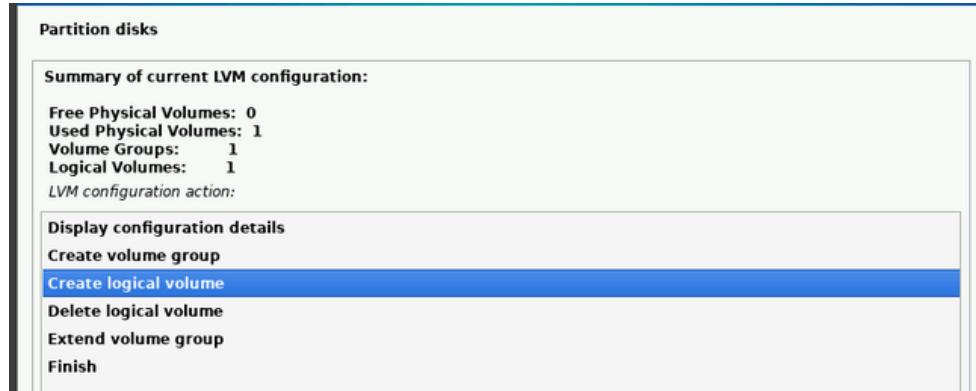


impostiamo la grandezza desiderata, **8192MB**

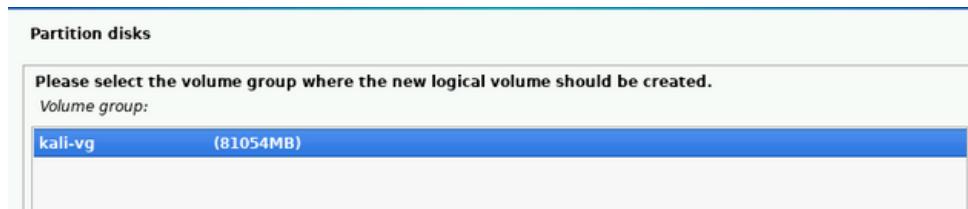


Creazione del volume logico **root**

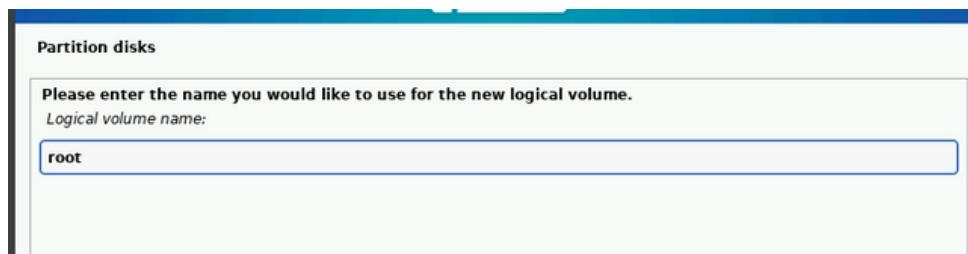
selezioniamo **Create logical volume**



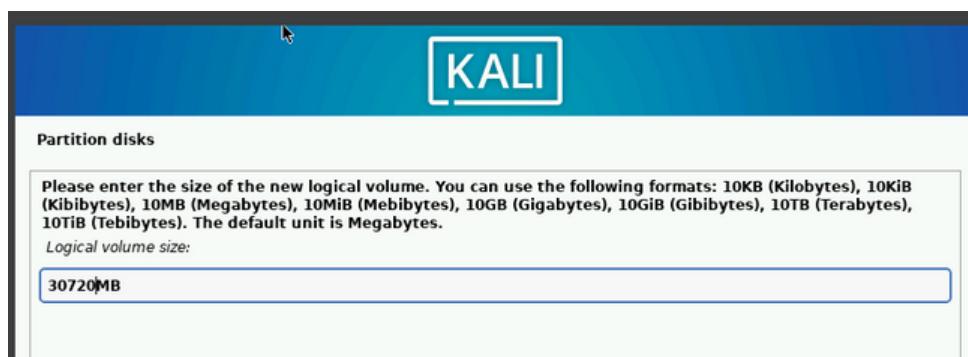
selezioniamo il **Volume Group**



inseriamo il nome del volume logico, **root**



impostiamo la grandezza desiderata, **30720MB**



Creazione del volume logico var

selezioniamo **Create logical volume**

Partition disks

Summary of current LVM configuration:

Free Physical Volumes: 0
Used Physical Volumes: 1
Volume Groups: 1
Logical Volumes: 2

LVM configuration action:

- Display configuration details
- Create volume group
- Create logical volume**
- Delete logical volume
- Extend volume group
- Finish

selezioniamo il **Volume Group**

Partition disks

Please select the volume group where the new logical volume should be created.

Volume group:

- kali-vg (81054MB)**

inseriamo il nome del volume logico, **var**

Partition disks

Please enter the name you would like to use for the new logical volume.

Logical volume name:

impostiamo la grandezza desiderata, **20480 MB**

Partition disks

Please enter the size of the new logical volume. You can use the following formats: 10KB (Kilobytes), 10KiB (Kibibytes), 10MB (Megabytes), 10MiB (Mebibytes), 10GB (Gigabytes), 10GiB (Gibibytes), 10TB (Terabytes), 10TiB (Tebibytes). The default unit is Megabytes.

Logical volume size:

Creazione del volume logico tmp

selezioniamo **Create logical volume**

Partition disks

Summary of current LVM configuration:

Free Physical Volumes: 0
Used Physical Volumes: 1
Volume Groups: 1
Logical Volumes: 3

LVM configuration action:

- Display configuration details
- Create volume group
- Create logical volume**
- Delete logical volume
- Extend volume group
- Finish

selezioniamo il **Volume Group**

Partition disks

Please select the volume group where the new logical volume should be created.

Volume group:

- kali-vg (29859MB)**

inseriamo il nome del volume logico, **tmp**

Partition disks

Please enter the name you would like to use for the new logical volume.

Logical volume name:

impostiamo la grandezza desiderata, **2048 MB**

Partition disks

Please enter the size of the new logical volume. You can use the following formats: 10KB (Kilobytes), 10KiB (Kibibytes), 10MB (Megabytes), 10MiB (Mebibytes), 10GB (Gigabytes), 10GiB (Gibibytes), 10TB (Terabytes), 10TiB (Tebibytes). The default unit is Megabytes.

Logical volume size:

Creiamo il volume logico finale per la directory **home**

selezioniamo **Create logical volume**

Partition disks

Summary of current LVM configuration:

Free Physical Volumes: 0
Used Physical Volumes: 1
Volume Groups: 1
Logical Volumes: 4

LVM configuration action:

Display configuration details
Create volume group
Create logical volume
Delete logical volume
Extend volume group
Finish

Selezioniamo nuovamente lo spazio libero nel Volume Group *kali-vg*,
Assegniamo il nome **home** e dedichiamo **tutto lo spazio rimanente** a questa partizione.

Partition disks

Please select the volume group where the new logical volume should be created.

Volume group:

kali-vg (27812MB)

inseriamo **home**

Partition disks

Please enter the name you would like to use for the new logical volume.

Logical volume name:

home

inseriamo **la grandezza desiderata**

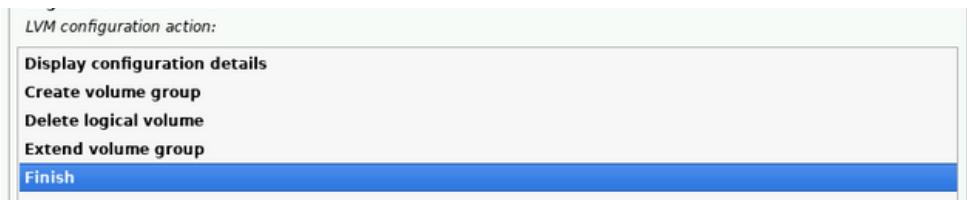
Partition disks

Please enter the size of the new logical volume. You can use the following formats: 10KB (Kilobytes), 10KiB (Kibibytes), 10MB (Megabytes), 10MiB (Mebibytes), 10GB (Gigabytes), 10GiB (Gibibytes), 10TB (Terabytes), 10TiB (Tebibytes). The default unit is Megabytes.

Logical volume size:

27812MB

selezioniamo **Finish**



selezionare **Finish partitioning and write changes to disk**

Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

Partition	Type	Size	File System	Mount Point
LVM VG kali-vg, LV home	Linux device-mapper (linear)	27.8 GB		
> #1		27.8 GB		
LVM VG kali-vg, LV root	Linux device-mapper (linear)	30.7 GB		
> #1		30.7 GB		
LVM VG kali-vg, LV swap	Linux device-mapper (linear)	8.2 GB		
> #1		8.2 GB		
LVM VG kali-vg, LV tmp	Linux device-mapper (linear)	2.0 GB		
> #1		2.0 GB		
LVM VG kali-vg, LV var	Linux device-mapper (linear)	20.5 GB		
> #1		20.5 GB		
Encrypted volume (sda2_crypt)	Linux device-mapper (crypt)	89.3 GB	K lvm	
> #1		89.3 GB	K lvm	
SCSI3 (0,0,0) (sda)	ATA VBOX HARDDISK	91.3 GB		
> #1 primary	ext4	2.0 GB	B F	/boot
> #2 primary	crypto	89.3 GB	K	(sda2_crypt)

Screenshot Help Go Back Continue

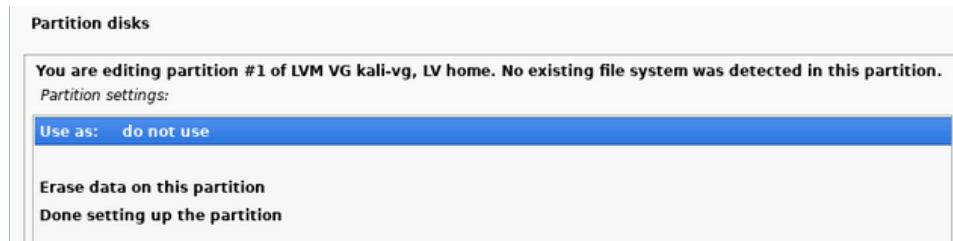
Terminata la configurazione **LVM**, selezioniamo '**Finish**' per completare la fase di partizionamento logico e procedere alla configurazione dei **mount point** per ciascun volume.

Impostiamo i **File System**, i **Mount Point** e le altre opzioni dei volumi Logici

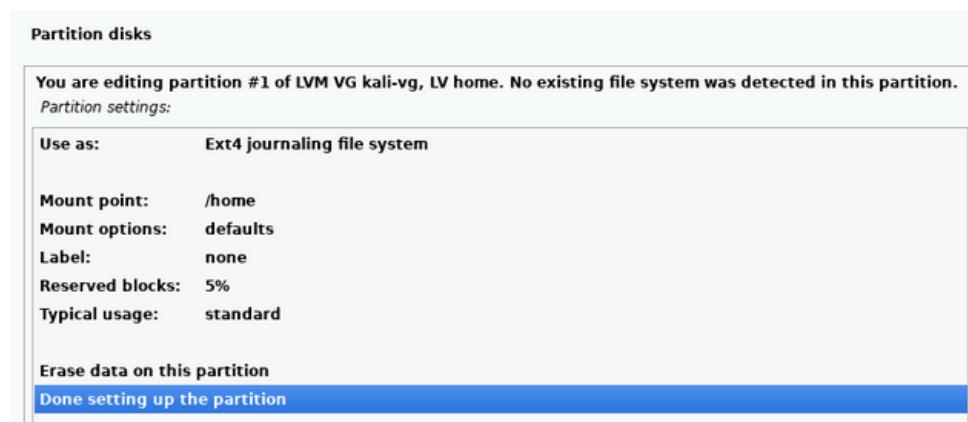
Cominciamo con **home**



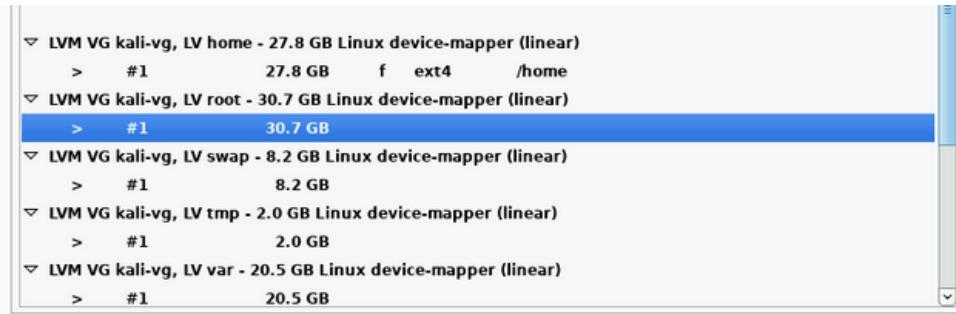
modifichiamo **Use as: do not use** in **Ext4 journaling file system**



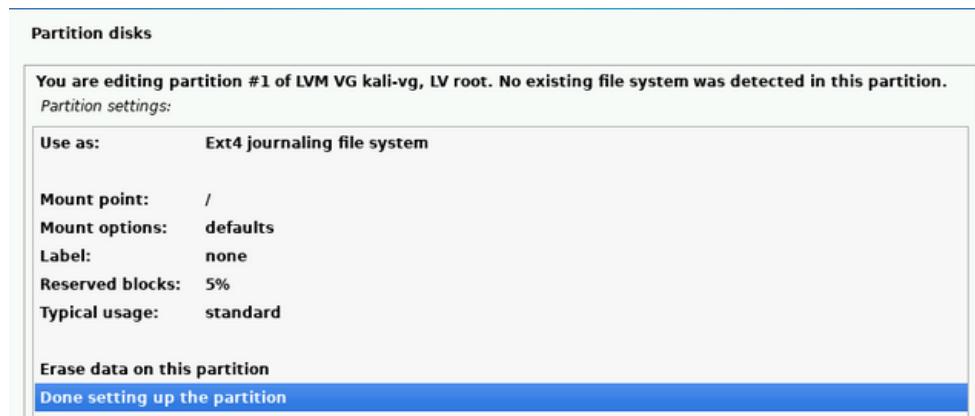
settiamo **Mount point:** a **/home**
selezioniamo **Done setting up the partition**



Impostiamo i File System, i Mount Point di Root



modifichiamo **Use as: do not use in Ext4 journaling file system**
settiamo il **Mount point a / - the root file system**

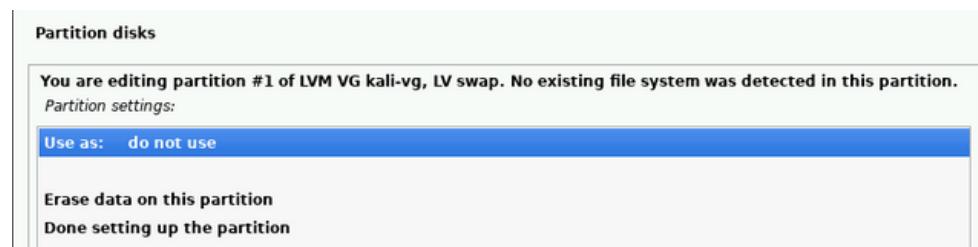


selezioniamo **Done setting up the partition**

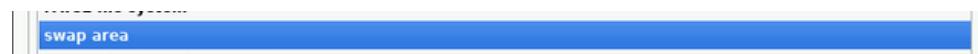
Impostiamo i File System, i Mount Point di swap

```
> LVM VG kali-vg, LV home - 27.8 GB Linux device-mapper (linear)
  > #1      27.8 GB   f  ext4    /home
> LVM VG kali-vg, LV root - 30.7 GB Linux device-mapper (linear)
  > #1      30.7 GB   f  ext4    /
> LVM VG kali-vg, LV swap - 8.2 GB Linux device-mapper (linear)
  > #1      8.2 GB
> LVM VG kali-vg, LV tmp - 2.0 GB Linux device-mapper (linear)
  > #1      2.0 GB
> LVM VG kali-vg, LV var - 20.5 GB Linux device-mapper (linear)
  > #1      20.5 GB
> Encrypted volume (sda2_crypt) - 89.3 GB Linux device-mapper (crypt)
  > #1      89.3 GB   K  lvm
> SCSI3 (0,0,0) (sda) - 91.3 GB ATA VBOX HARDDISK
  > #1  primary    2.0 GB   B  F  ext4    /boot
  > #2  primary    89.3 GB   K  crypto   (sda2_crypt)
```

modifichiamo **Use as: do not use**

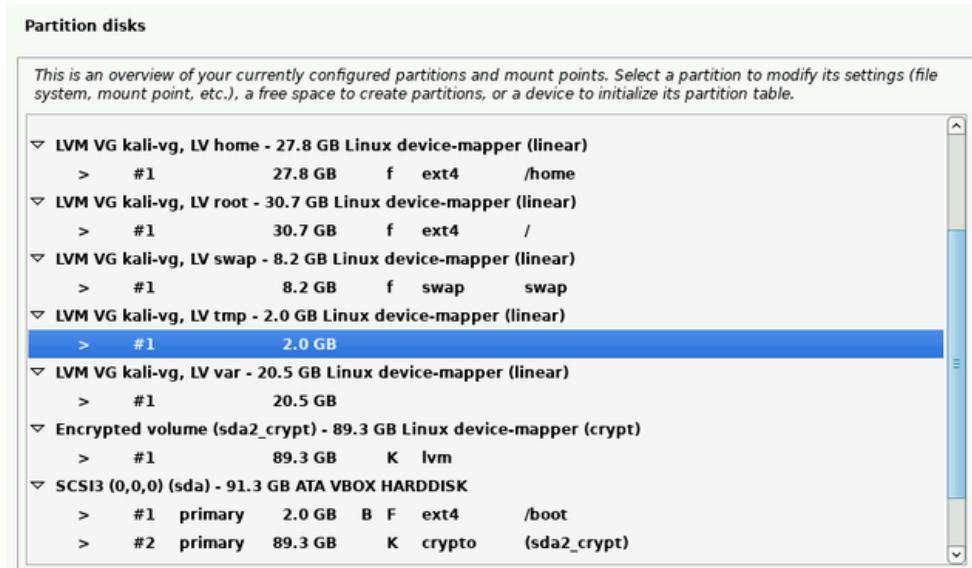


selezioniamo **swap area**

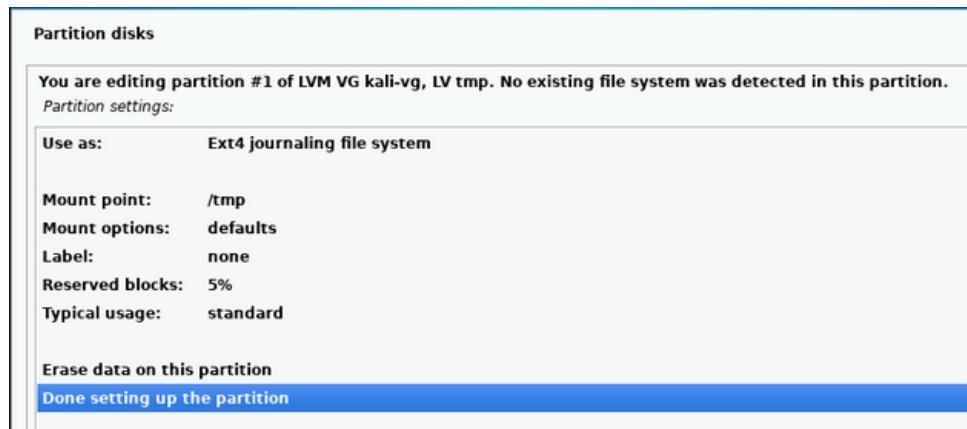


selezioniamo **Done setting up the partition**

Impostiamo i File System, i Mount Point di tmp



modifichiamo **Use as:** do not use in Ext4 journaling file system
settiamo il **Mount point** a /temp



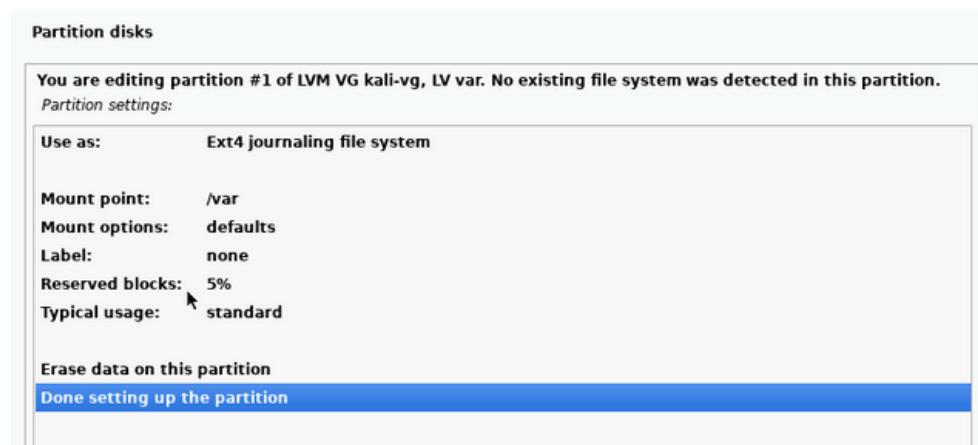
selezioniamo **Done setting up the partition**

Impostiamo i File System, i Mount Point di var

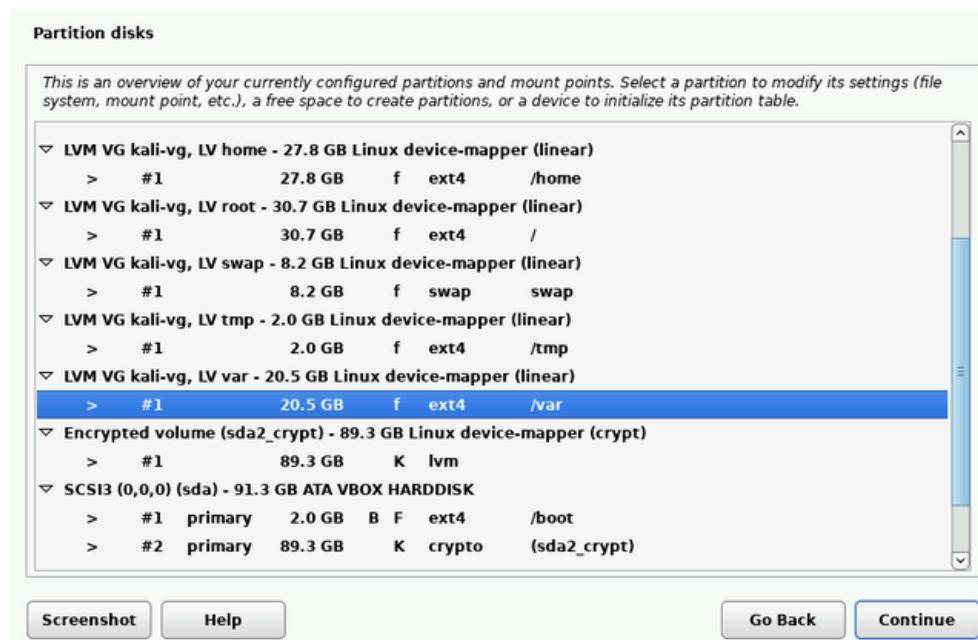
The screenshot shows the GParted partition editor interface. A tree view on the left lists partitions under 'LVM VG kali-vg'. The '/var' partition is selected and highlighted with a blue bar at the bottom. Its details are shown in the main pane:

- LVM VG kali-vg, LV root - 30.7 GB Linux device-mapper (linear)
- > #1 30.7 GB f ext4 /
- LVM VG kali-vg, LV swap - 8.2 GB Linux device-mapper (linear)
- > #1 8.2 GB f swap swap
- LVM VG kali-vg, LV tmp - 2.0 GB Linux device-mapper (linear)
- > #1 2.0 GB f ext4 /tmp
- LVM VG kali-vg, LV var - 20.5 GB Linux device-mapper (linear)
- > #1 20.5 GB
- Encrypted volume (sda2_crypt) - 89.3 GB Linux device-mapper (crypt)
- > #1 89.3 GB K lvm
- SCSI3 (0,0,0) (sda) - 91.3 GB ATA VBOX HARDDISK
- > #1 primary 2.0 GB B F ext4 /boot
- > #2 primary 89.3 GB K crypto (sda2_crypt)

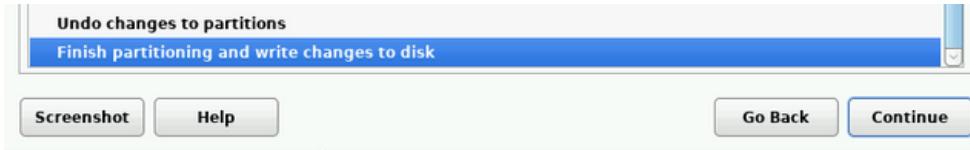
modifichiamo **Use as: do not use in Ext4 journaling file system**
settiamo il **Mount point** a **/var**



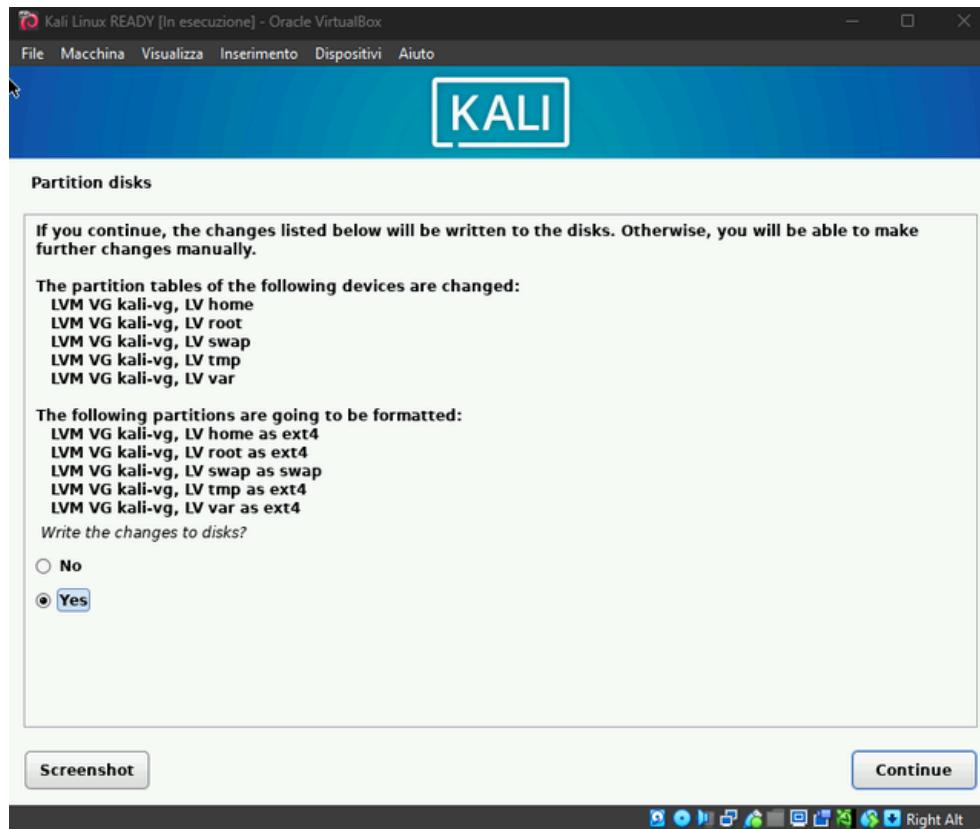
selezioniamo **Done setting up the partition**

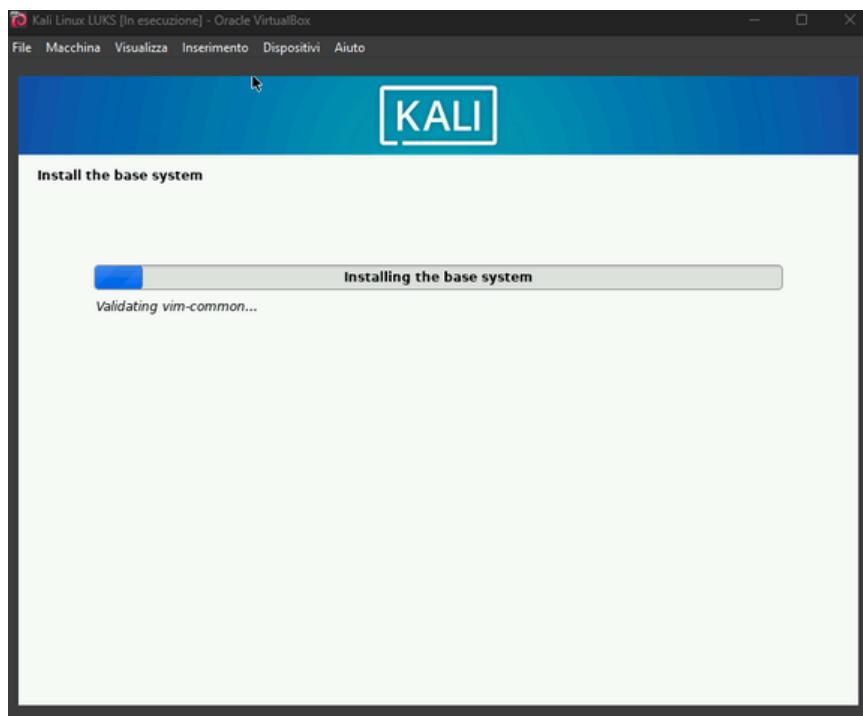


Una volta impostate le unita' logiche
selezioniamo **Finish partitioning and write changes to disk**

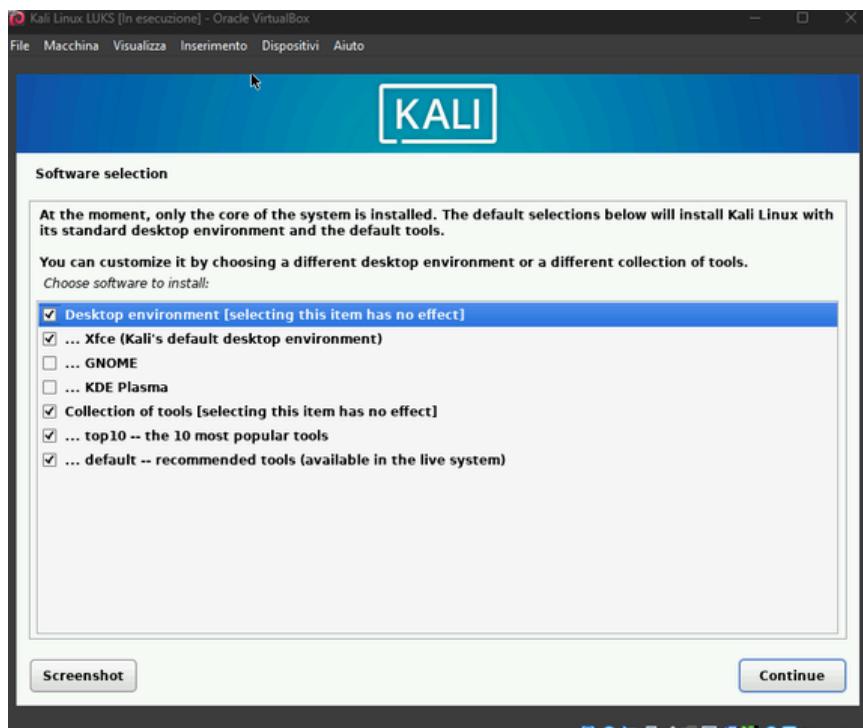


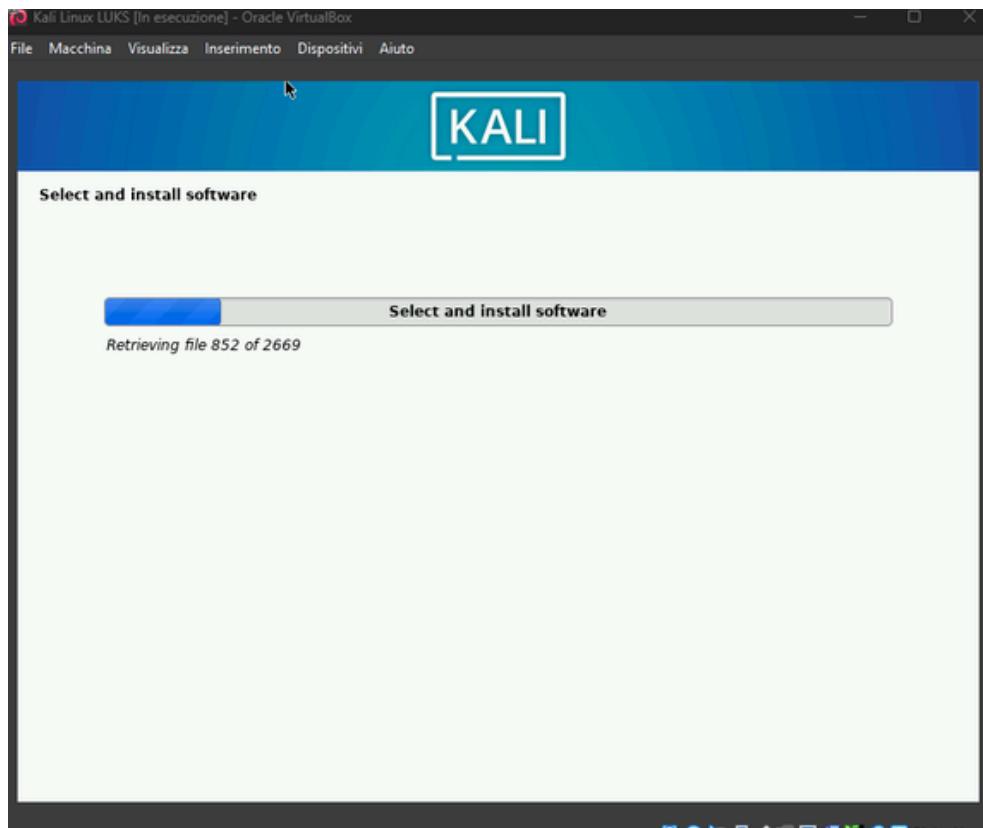
confermiamo con **YES**



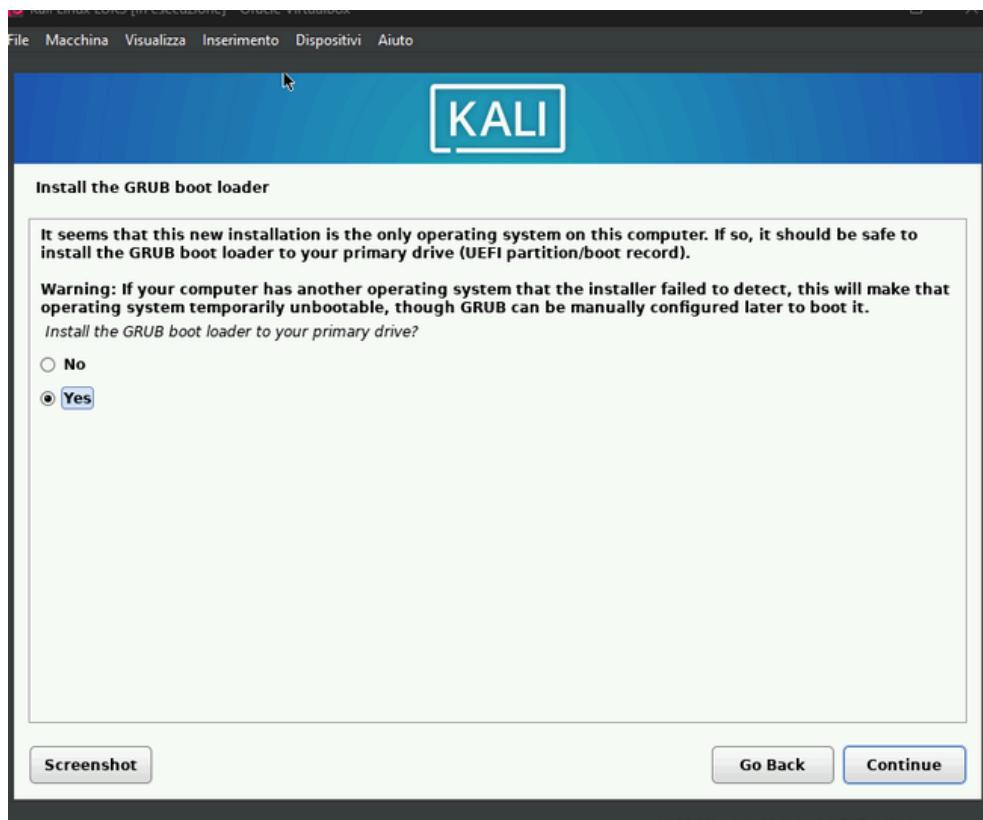


selezionare i **contenuti** da installare

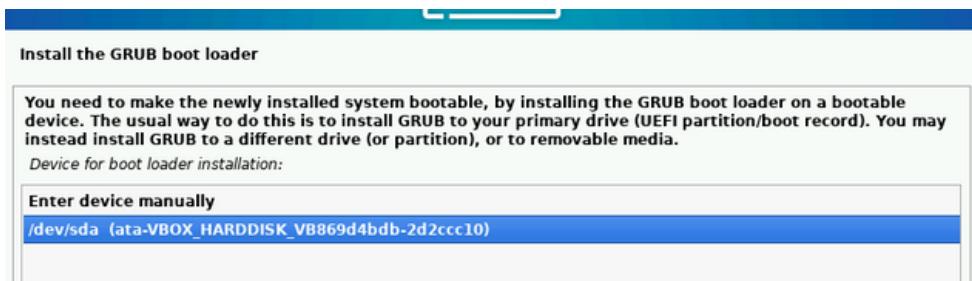




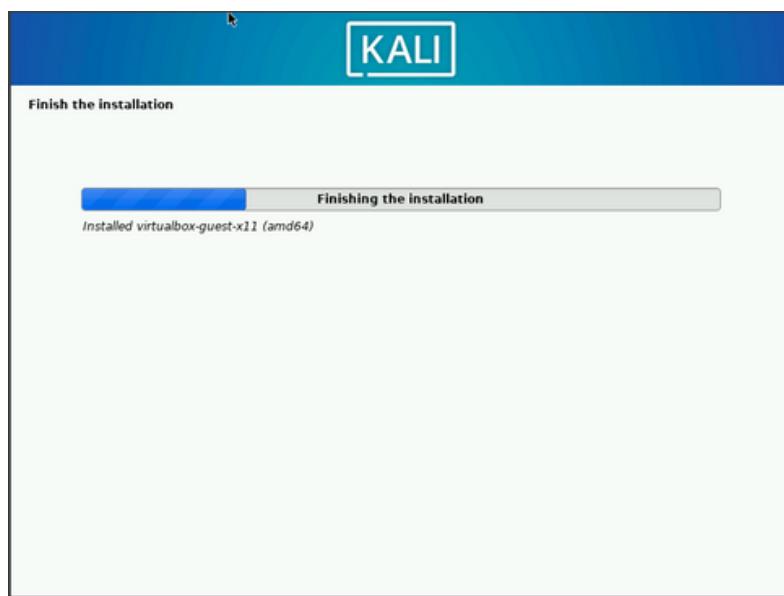
confermiamo con **yes**



selezioniamo il disco principale (**/dev/sda**) per l'installazione di **GRUB**



attendere il completamento



*al termine riavviare per completare l'installazione di Kali Linux con standard di crittografia del disco linux **LUKS attivo***



*inserire la **passphrase** creata precedentemente per sbloccare il disco rigido*

