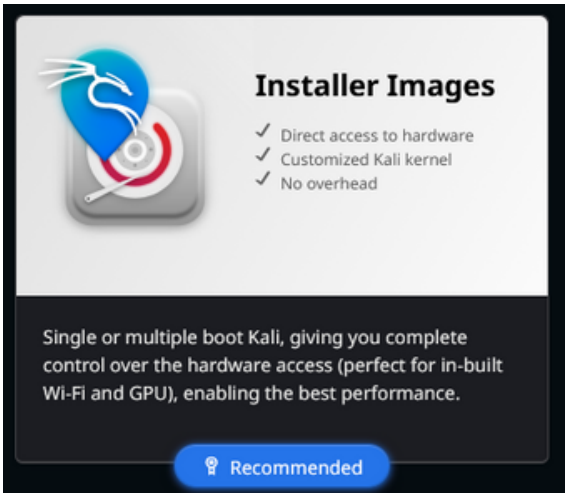
Installazione con partizione Criptata LUKS con suddivisione granulare delle partizioni

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.

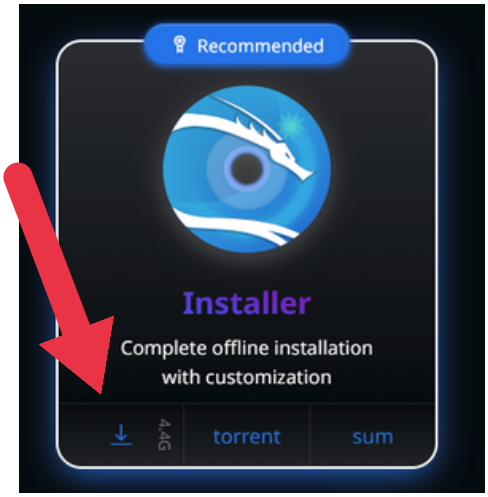
Un professionista **prevede e anticipa** i possibili **problemi** e complicazioni mettendo in atto misure per ridurre l'inpatto o evitarli.
Criptare il disco sfruttando il **LUKS** e' una buona pratica di sicurezza.

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**

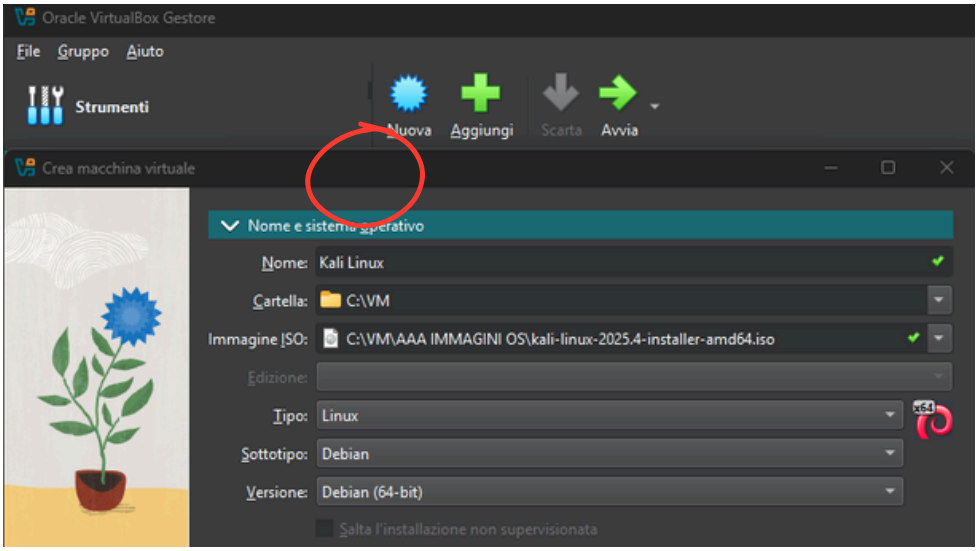
Da **Kali.org** andiamo nella sezione **download** e selezioniamo **Installer Images**



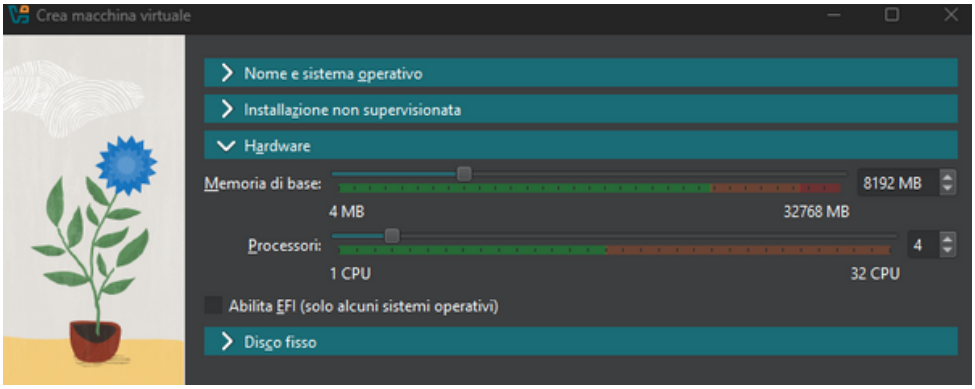
Click sul **link** per scaricare **ISO**



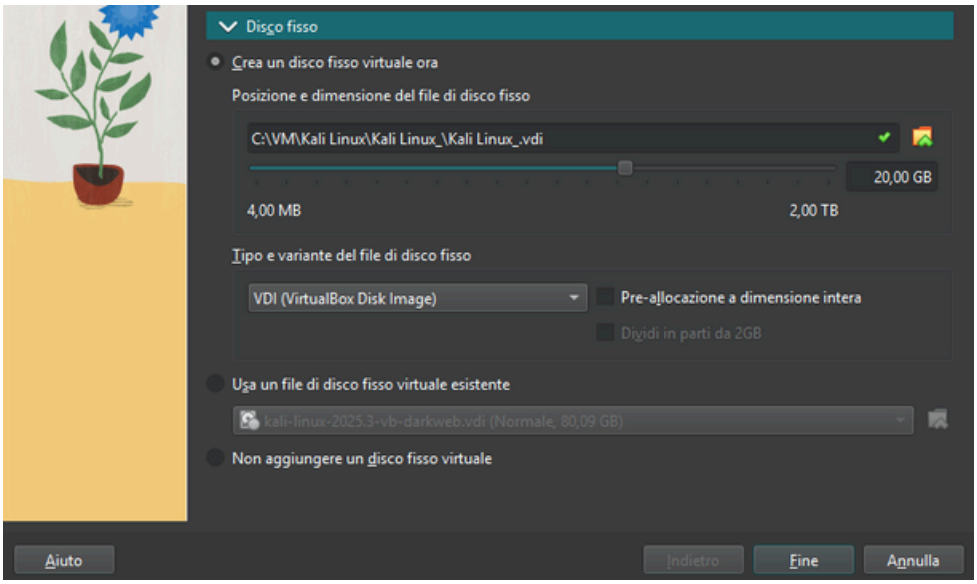
Da **Virtual Box,** selezioniamo **Nuova**
impostiamo **nome**, **cartella**, **immagine ISO**, **tipo**, **sottotipo** e **Versione**



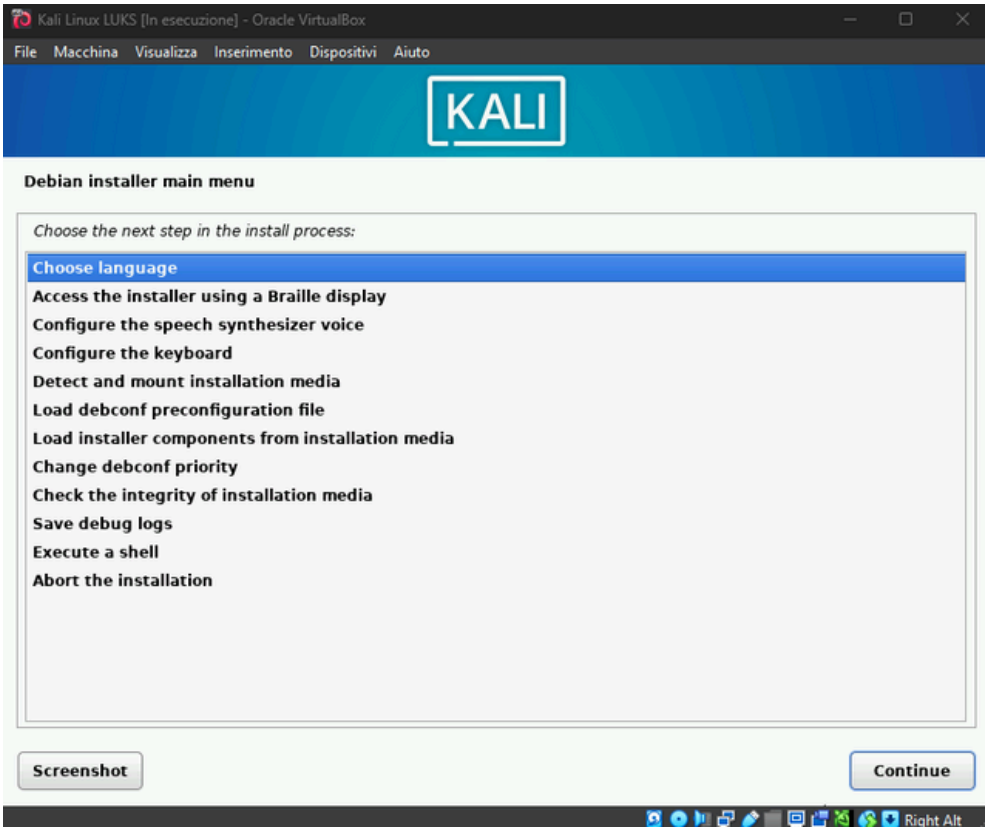
Configuriamo **la macchina virtuale** in base alle **nostre risorse**

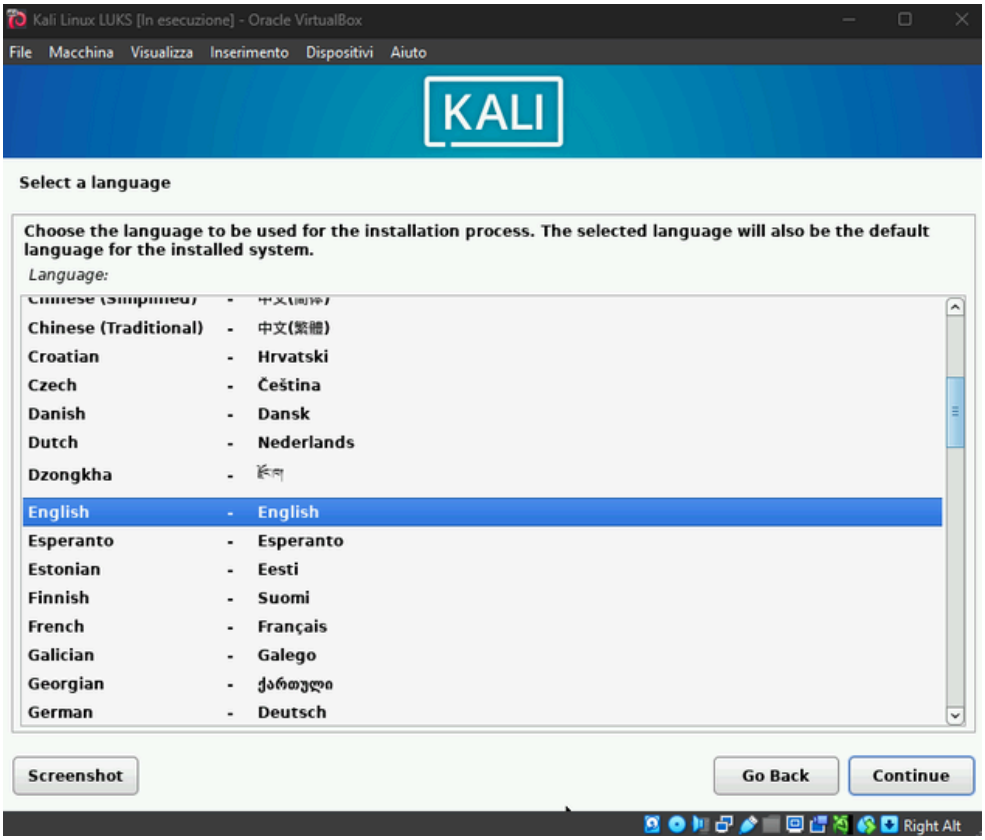


Scegliere la **dimensione** del **harddisk** desiderato

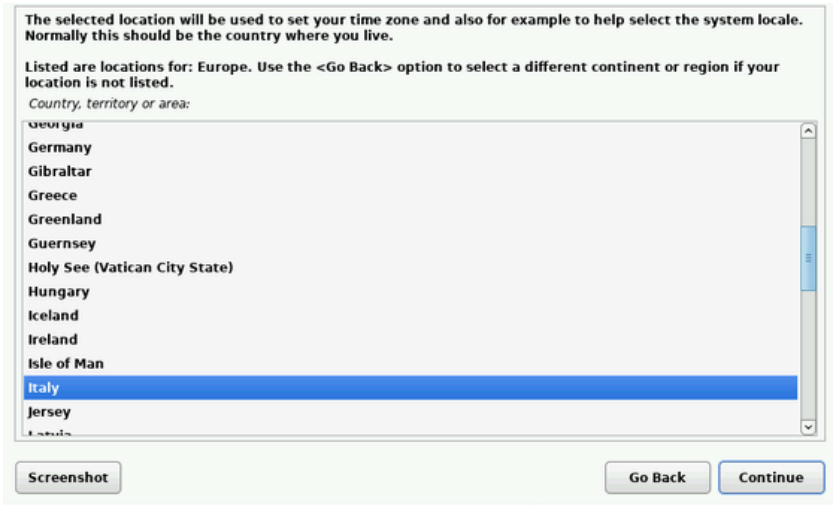


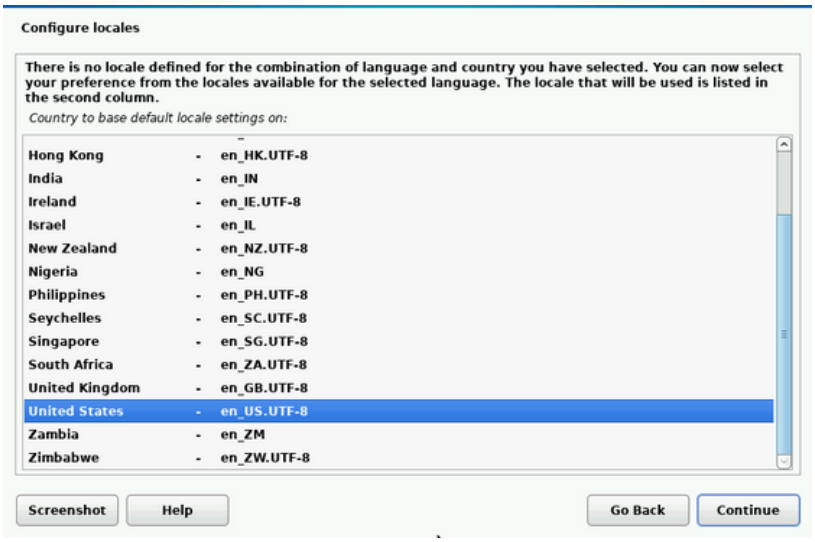
Selezioniamo la **lingua**



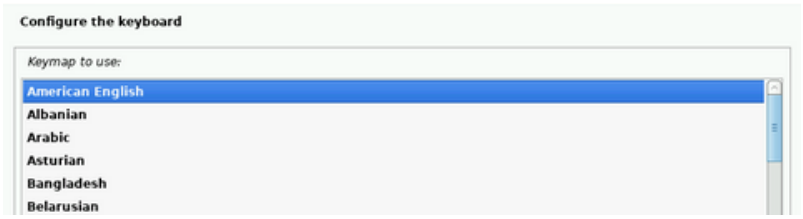


Selezioniamo il **paese** desiderato per avere le **opzioni relative**



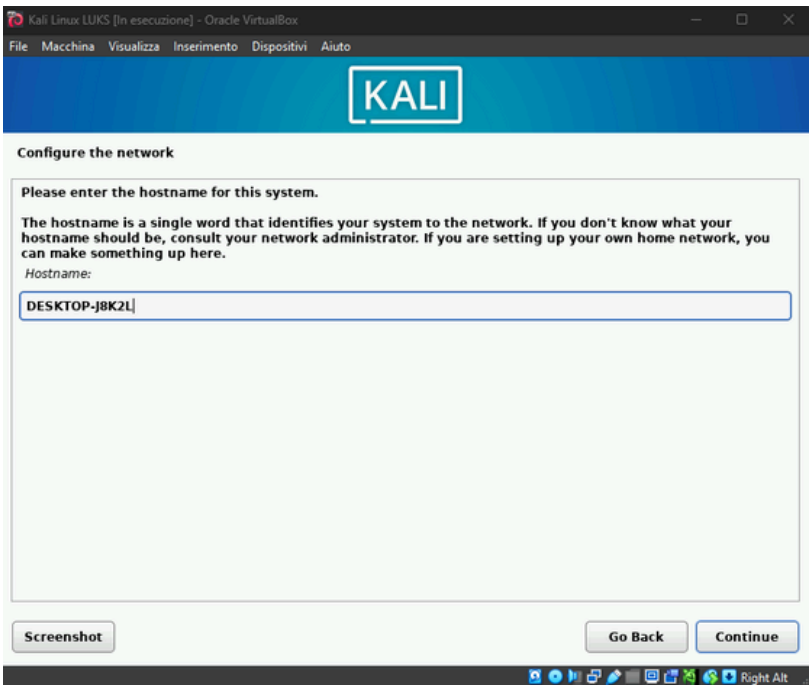


selezioniamo la **lingua** della **tastiera**

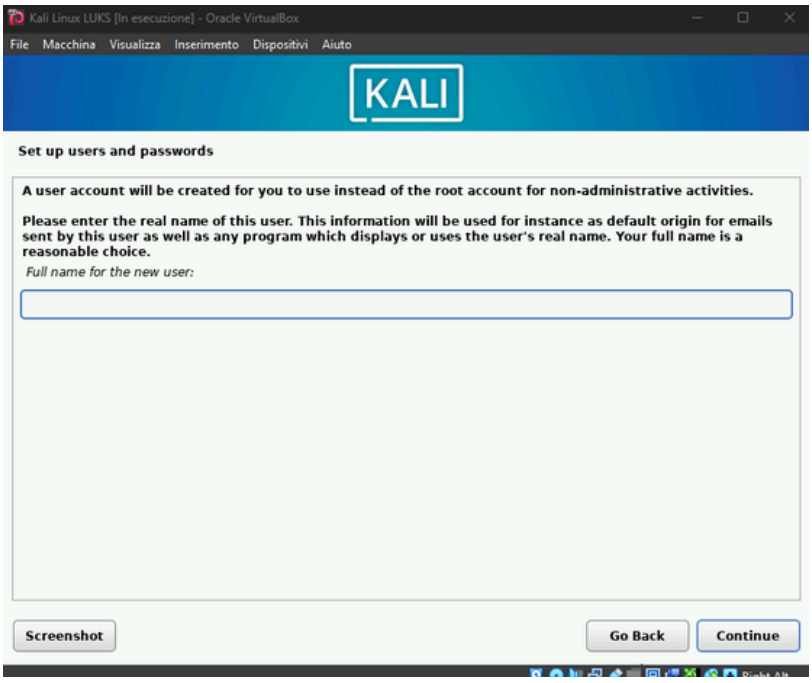


Configuriamo un hostname **generico** per dare meno nel occhio.
Esempi di nomi **HOST** di dispositivi **comuni**

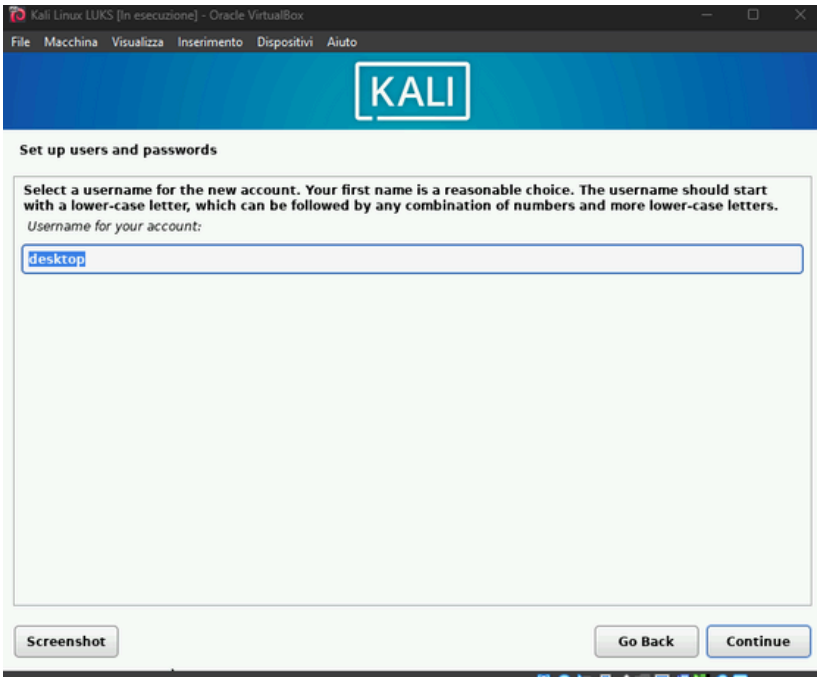
- Apple: **iPhone-di-Antonio**, **iPad-Air**..
- Windows: **DESKTOP-5A8F9**, **LAPTOP-8J2K1**..
- Altri: **Galaxy-S24**, **HPLaserJet-400**, **android-f82a9**..



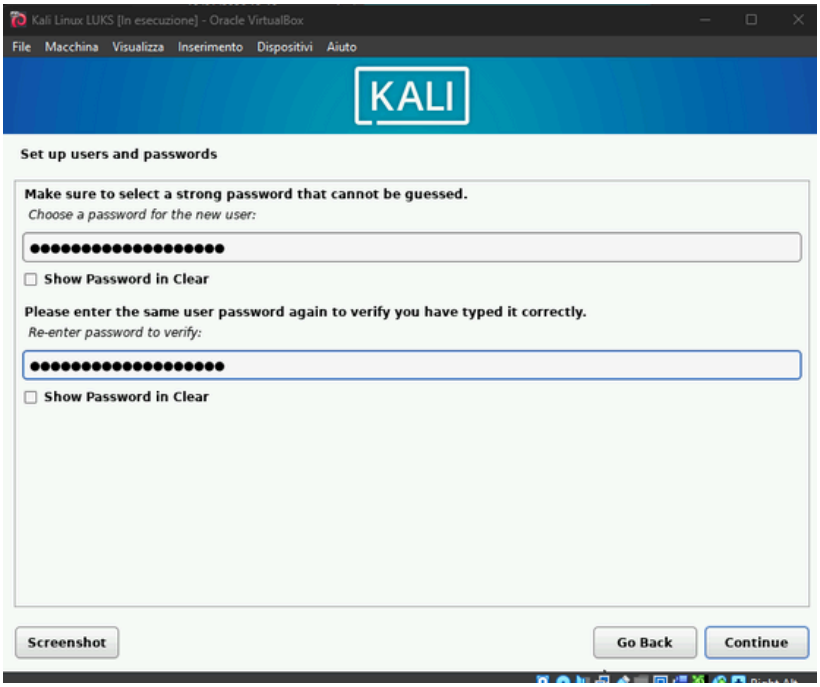
Cerchiamo di rimanere coerenti nei nomi o lasciarli vuoti

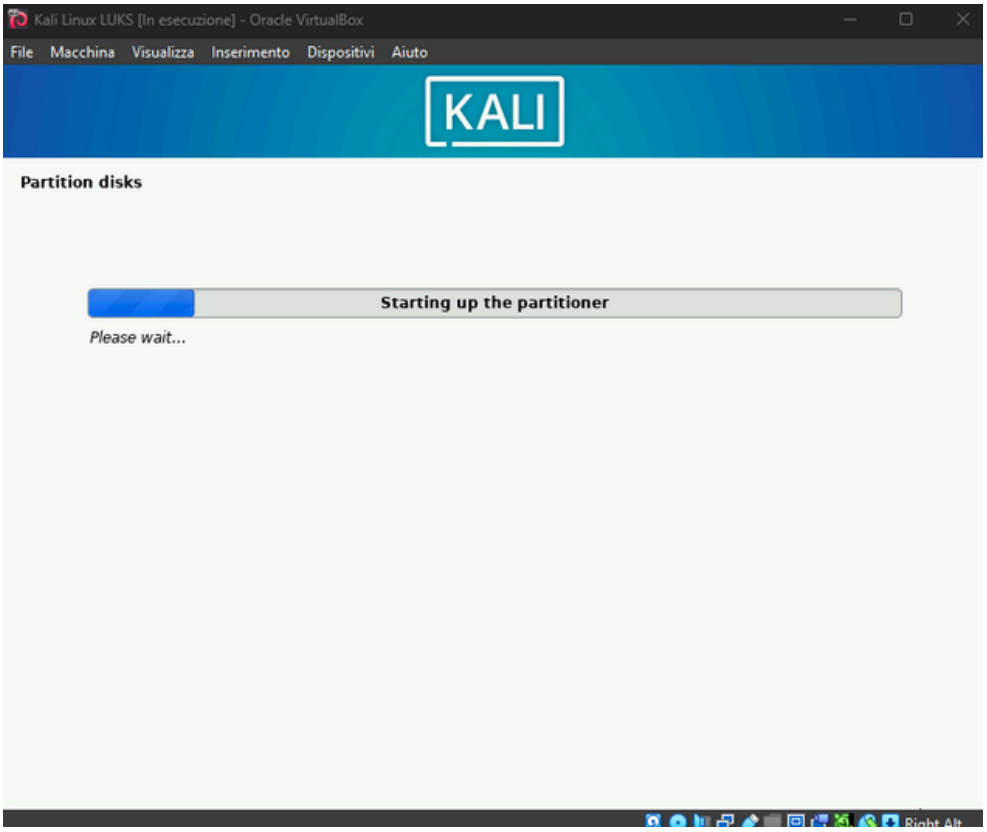


Inseriamo il **nome utente**

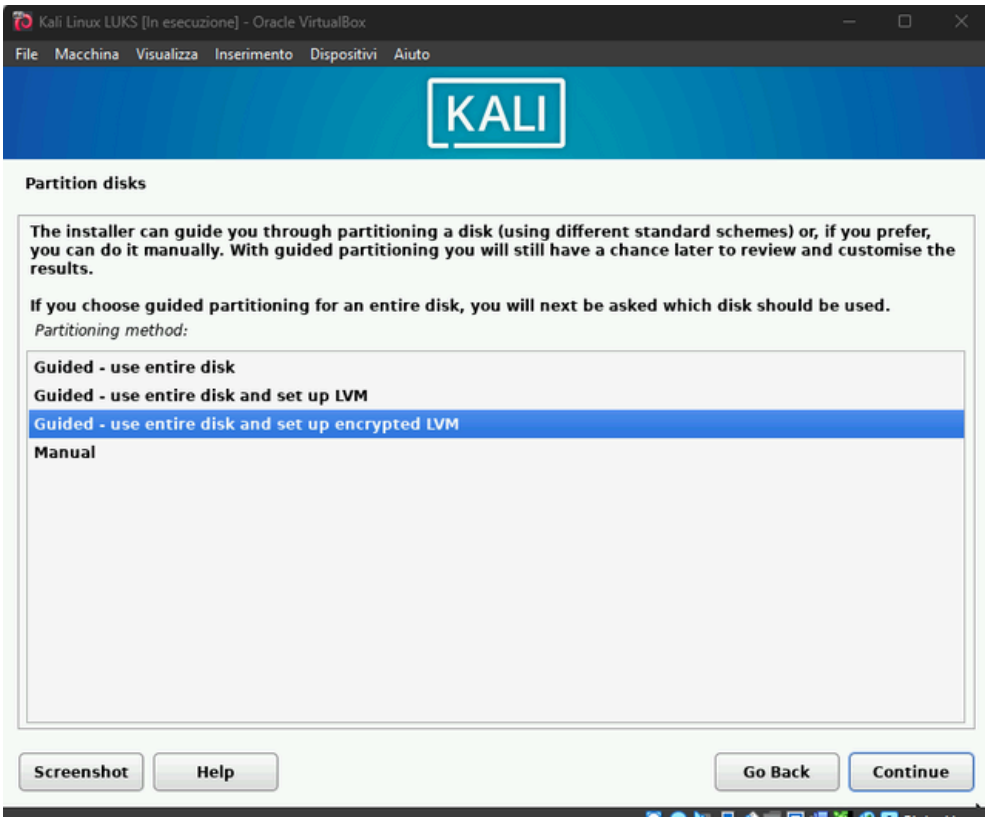


Generare una **passphrase** tra **16** e **30** caratteri.
La forza della **passphrase** e' la sua **lunghezza** e a come **viene gestita**

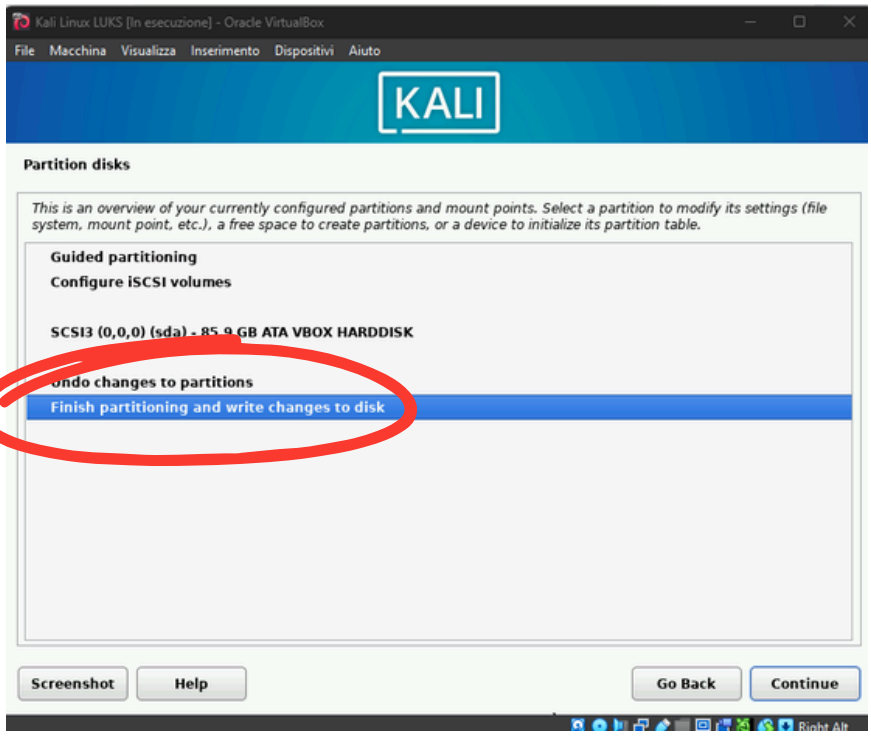




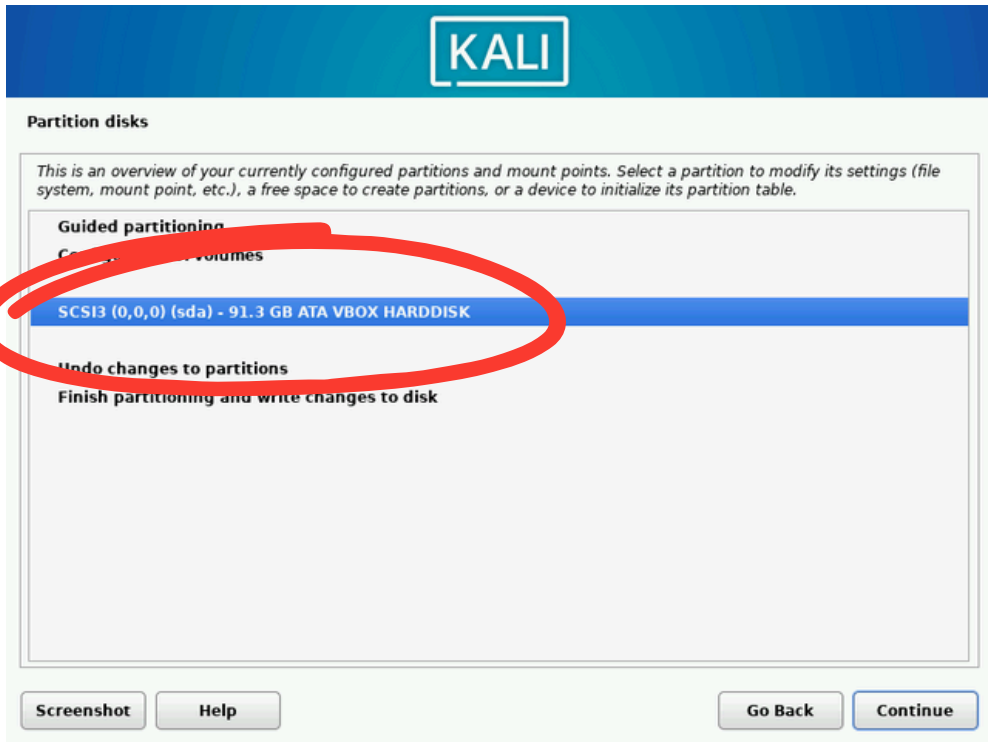
seleziona **Guided - use entire disk and set up encypted LVM**



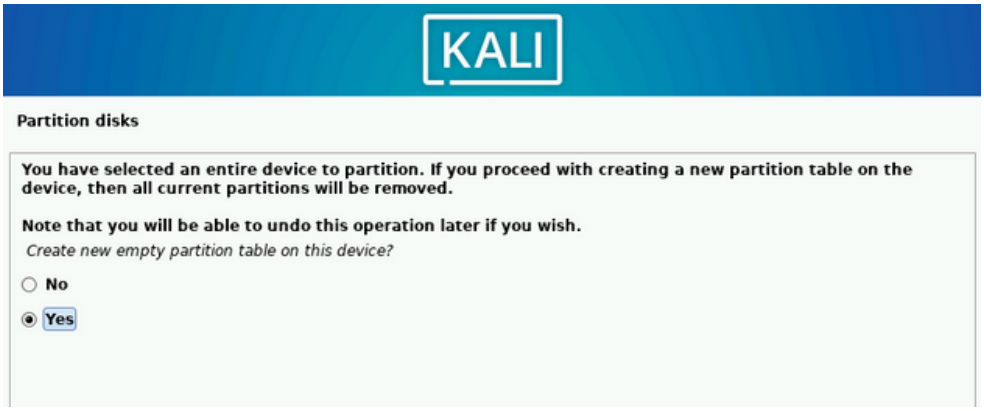
Finish partitioning and write changes to disk per lasciare il partizionamento automatico, tutto in una partizione



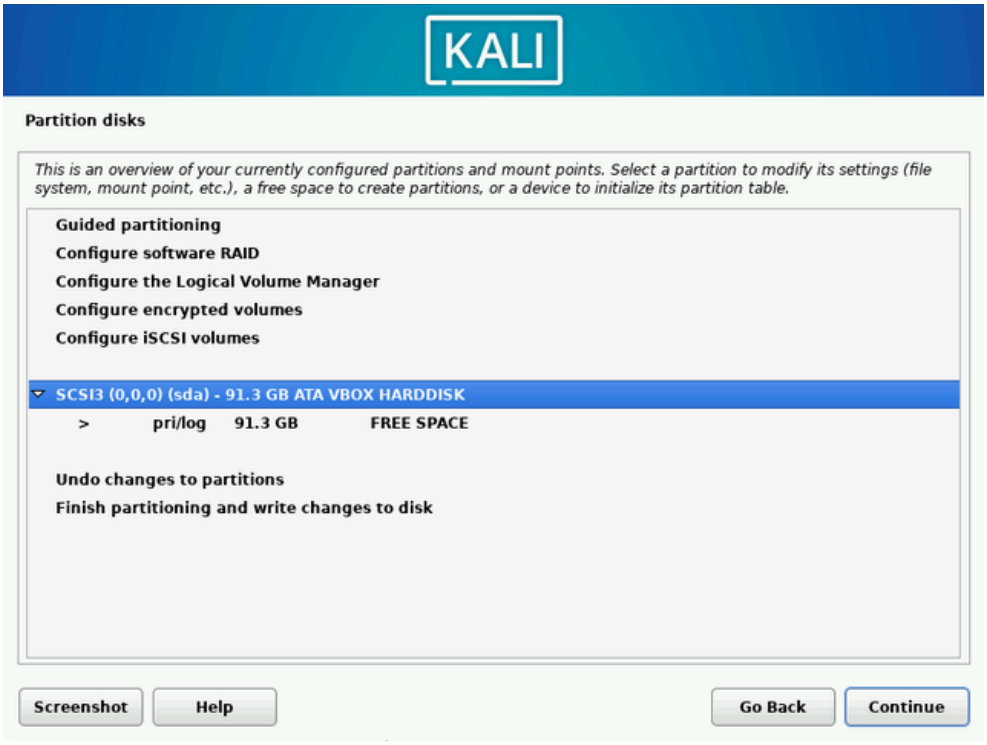
se vogliamo partizionare manualmente il disco selezioniamo **SCSI3 (0,0,0) - 91.3 GB ATA VBOX HARDDISK**



confermiamo con **YES**

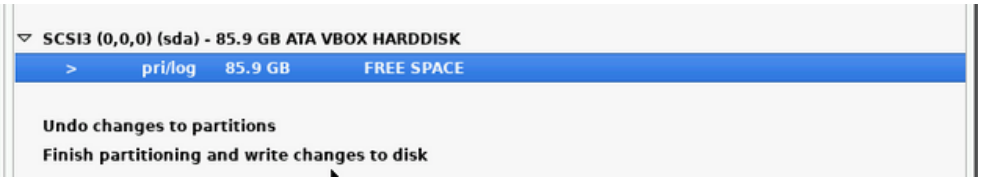


al termine avremo questa schermata riassuntiva della situazione

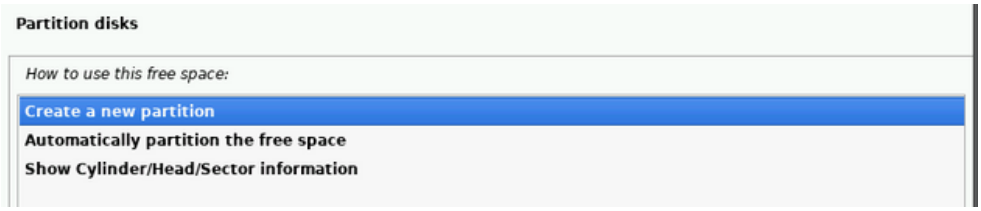


Creazione partizione di boot

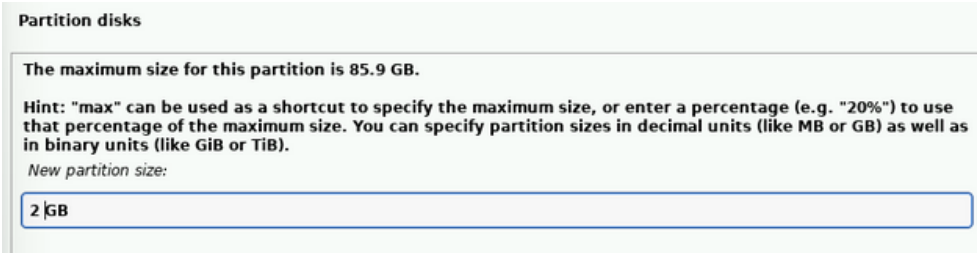
selezioniamo **FREE SPACE**



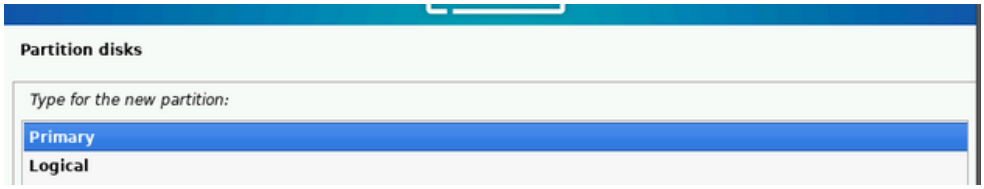
selezioniamo **Create a new partition**



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

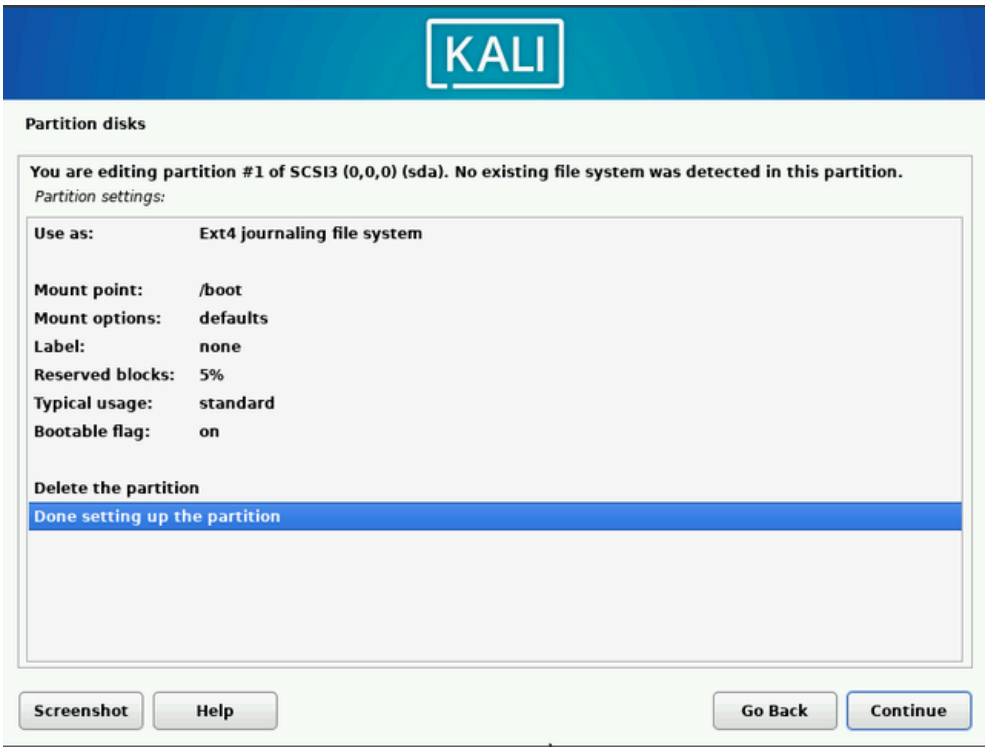


selezioniamo **Primary**



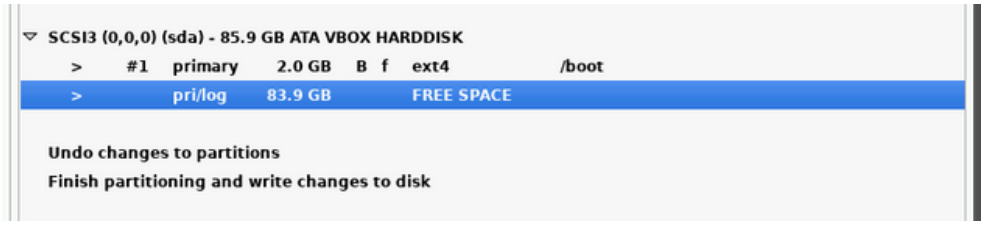
selezioniamo **Beginning**

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

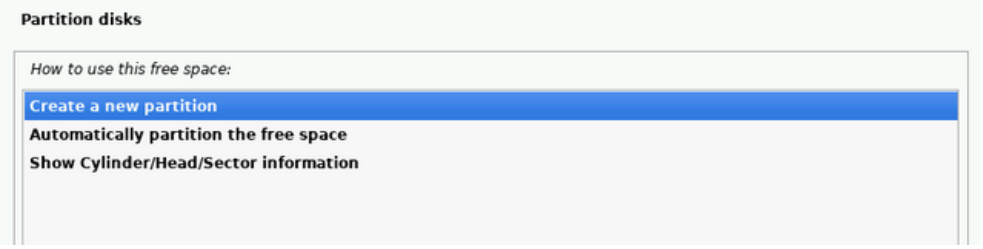


Creiamo la partizione che conterra' il volume cifrato

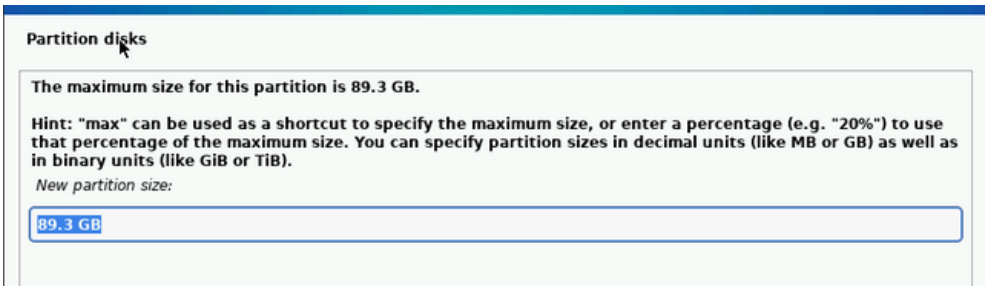
selezioniamo **FREE SPACE**



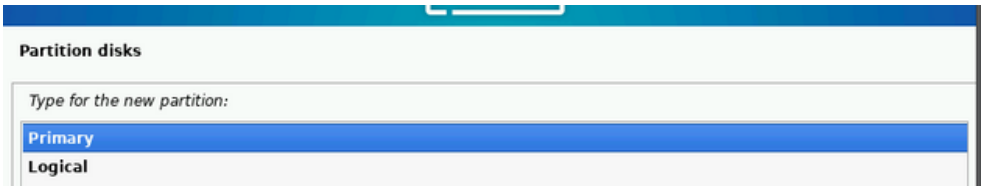
selezioniamo **Create a new partition**



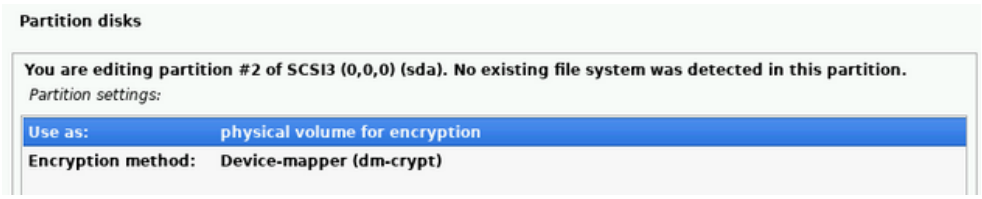
selezioniamo lo **spazio rimasto** che **diventera'** la nostra **cassaforte cifrata**



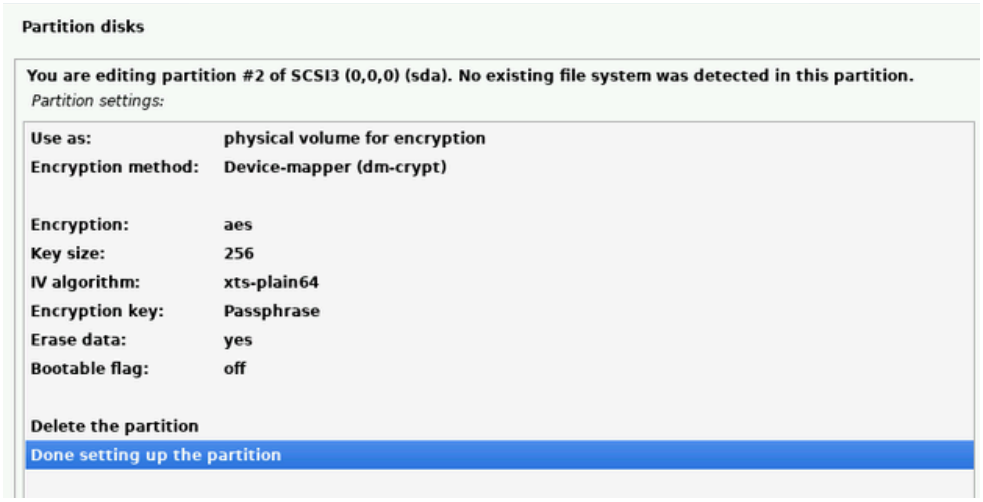
selezioniamo **Primary**



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

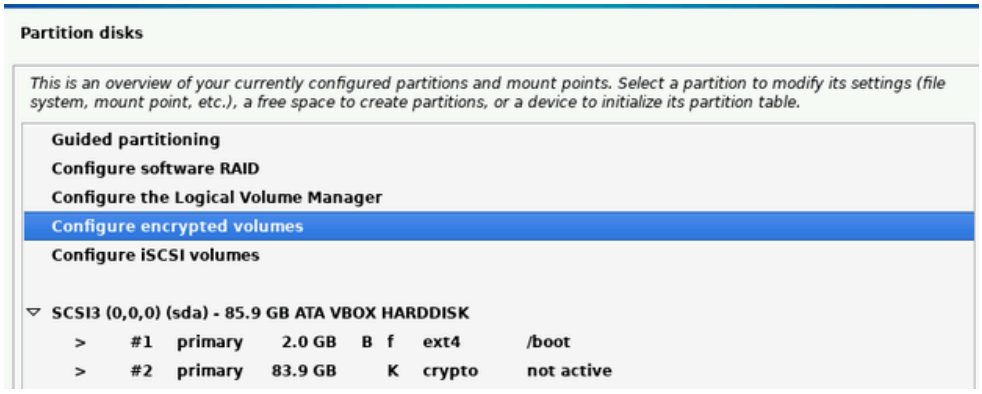


selezioniamo **Done setting up the partition**

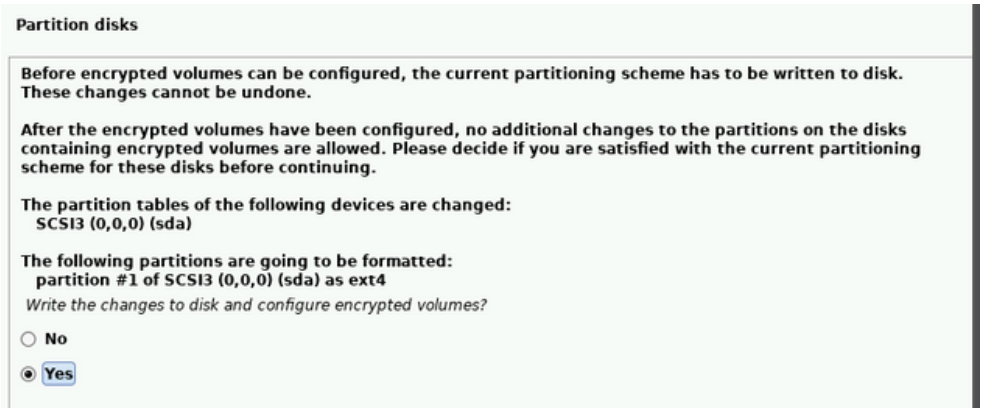


configuriamo il volume criptato

selezioniamo **Configure encrypted volumes**

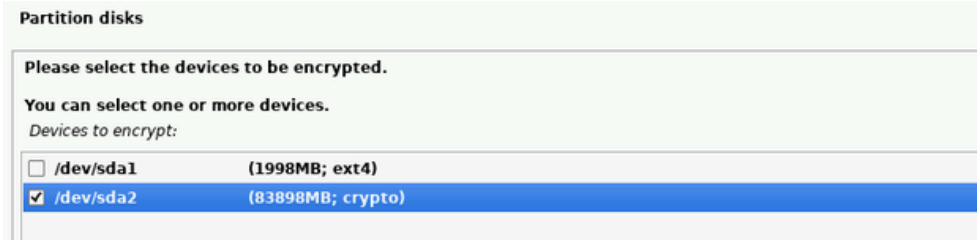


selezioniamo **Yes**

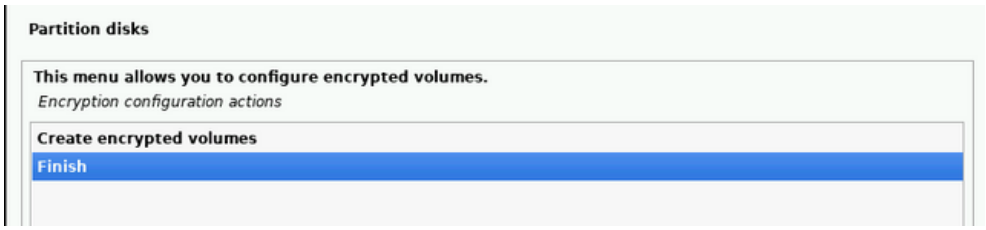


selezioniamo **Create encrypted volumes**

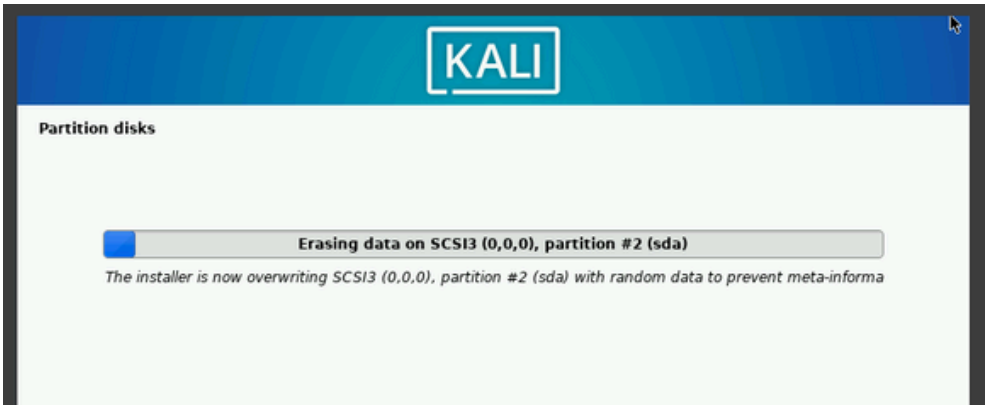
selezioniamo **/dev/sda2 (83898MB; crypto)**



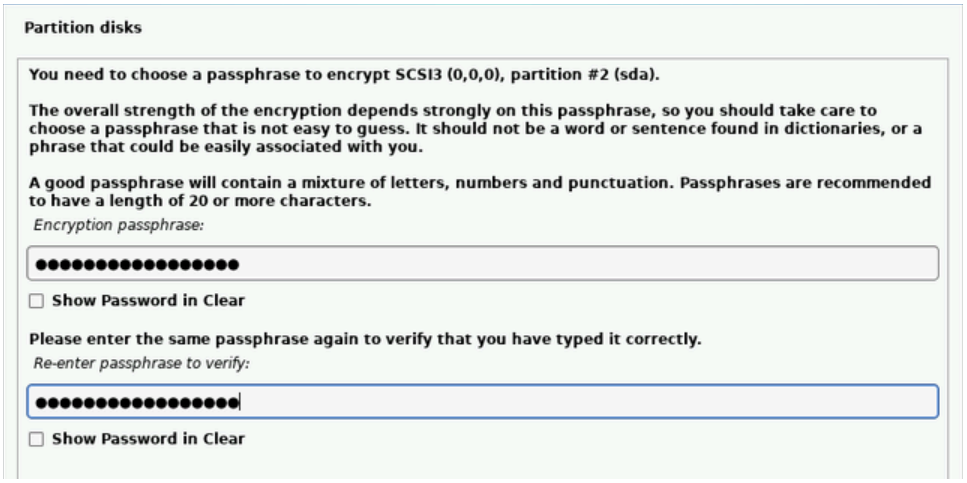
selezioniamo **Yes** e poi **Finish**



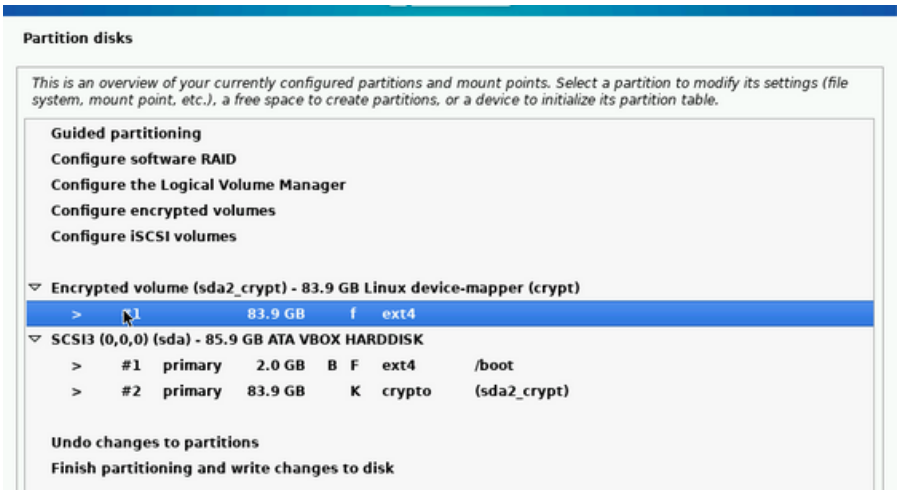
Attendiamo il completamento. Prima di inizializzare il volume cifrato, l'installer sovrascrive l'intero disco con dati casuali (misura anti-forense).



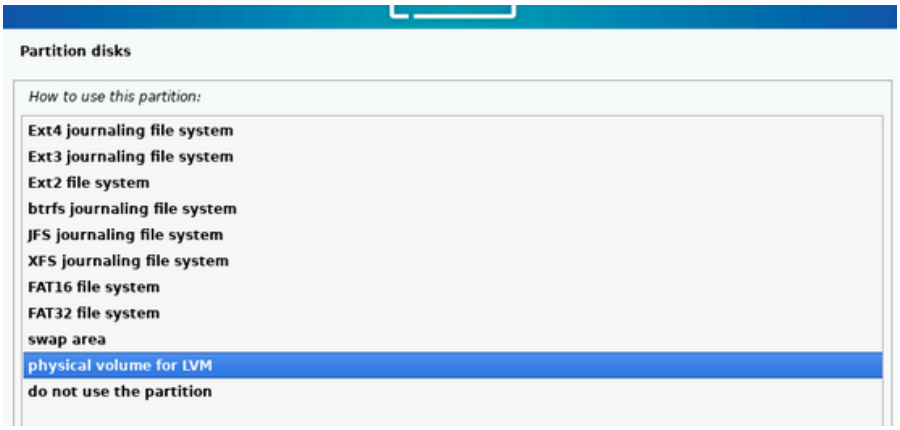
inserire la **passphrase** che **sblocchera' il disco rigido** all'accensione



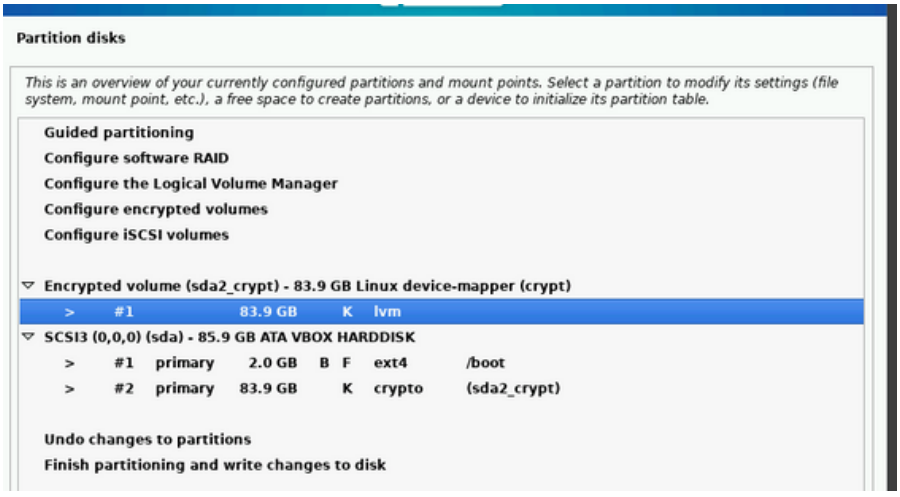
selezioniamo il volume **sda2_crypt** *per cambiarlo in volume fisico*



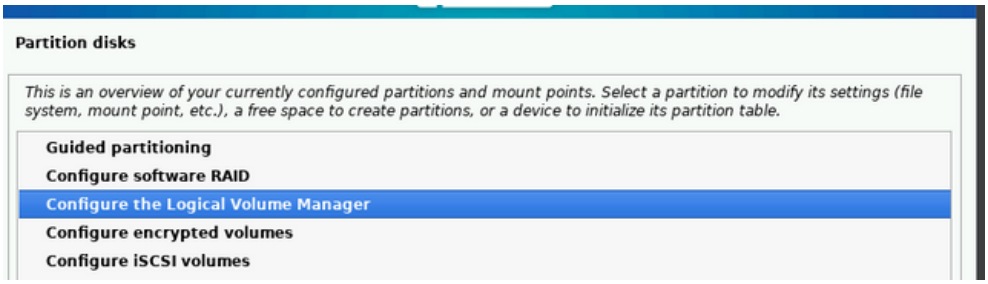
selezioniamo **physical volume for LVM**



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

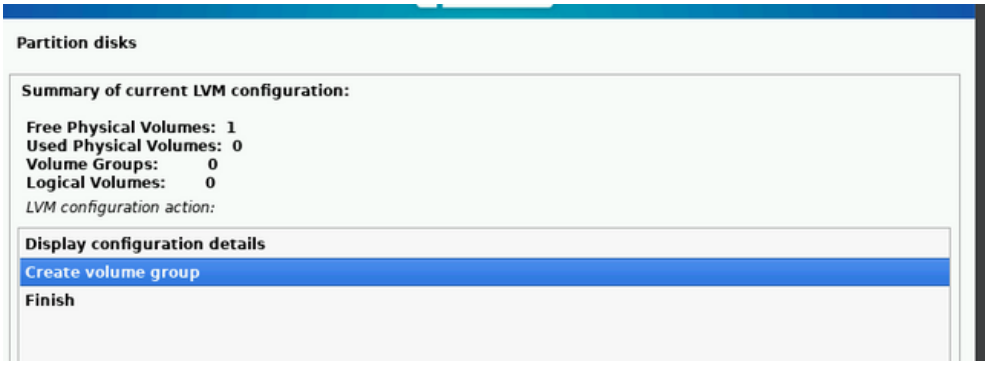


configuriamo il volume logico
selezioniamo **Configure the Logical Volume Manager**

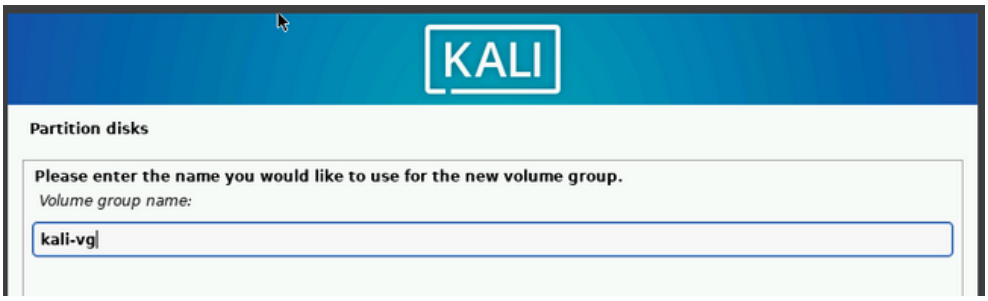


confermiamo con **Yes**

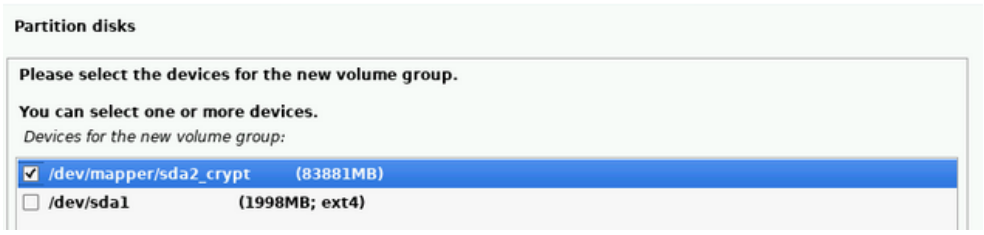
selezioniamo **Create volume group**



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



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

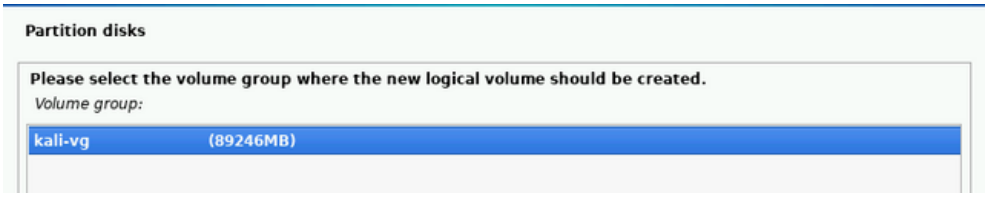


*Una volta creato il **Volume Group** andiamo a creare i **Volumi Logici.***

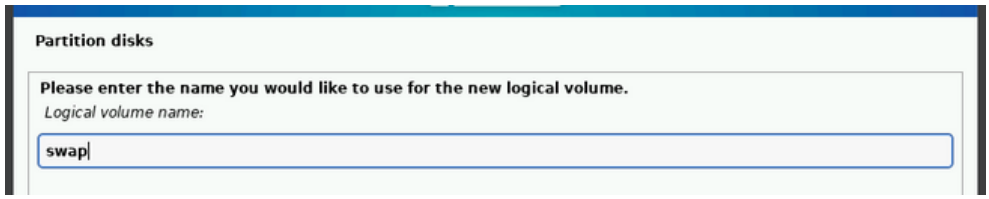
Creazione del volume logico **swap**

selezioniamo **Create logical volume**

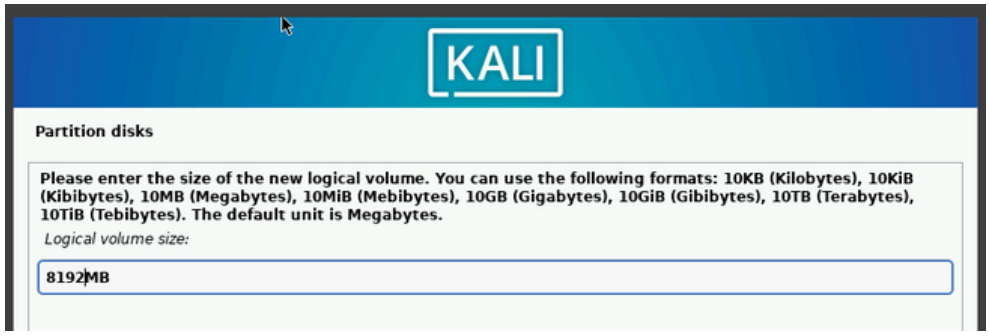
selezioniamo il **Volume Group**



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

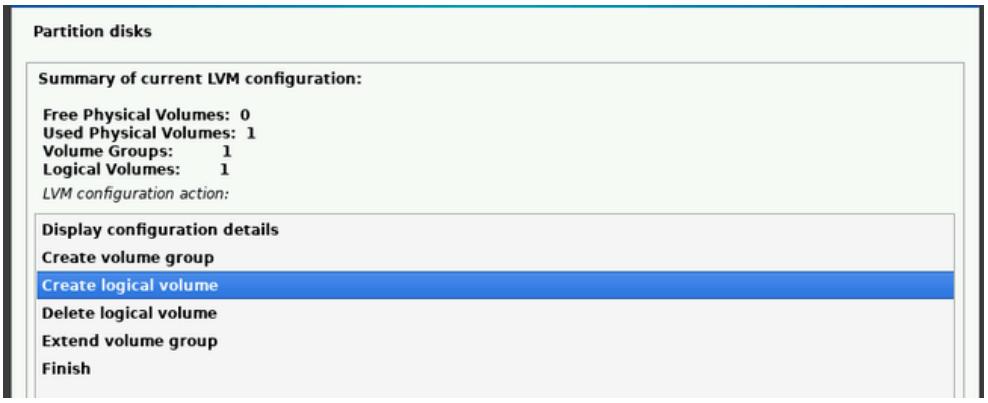


impostiamo la grandezza desiderata, **8192MB**

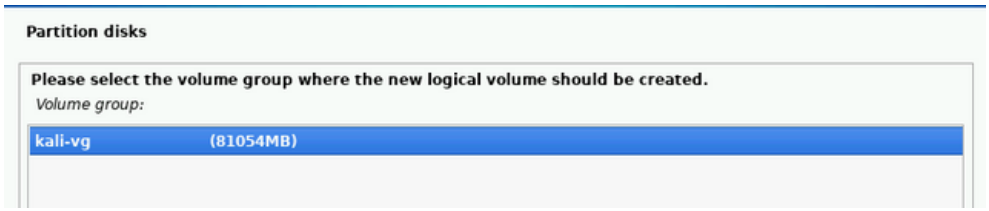


Creazione del volume logico **root**

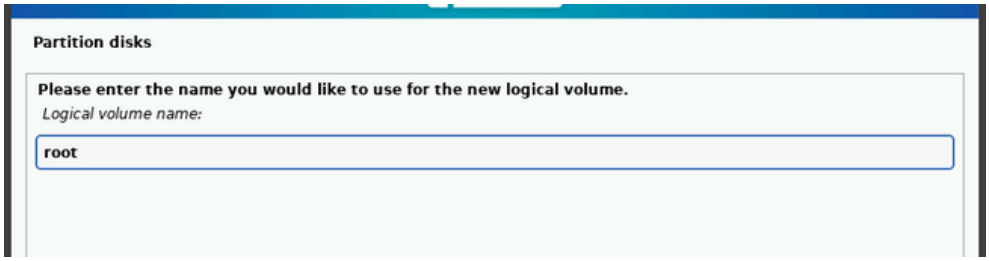
selezioniamo **Create logical volume**



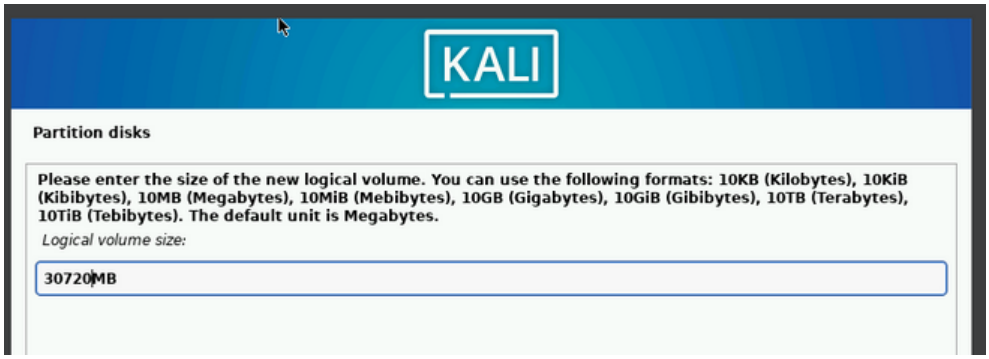
selezioniamo il **Volume Group**



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



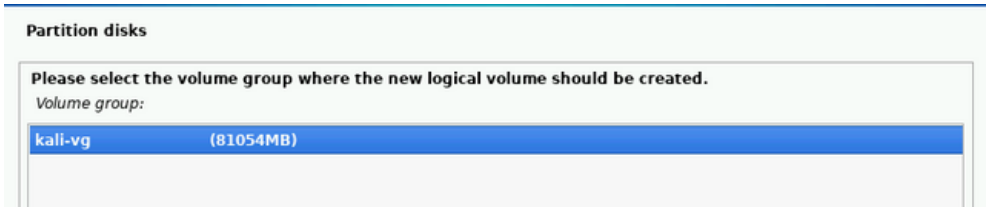
impostiamo la grandezza desiderata, **30720MB**



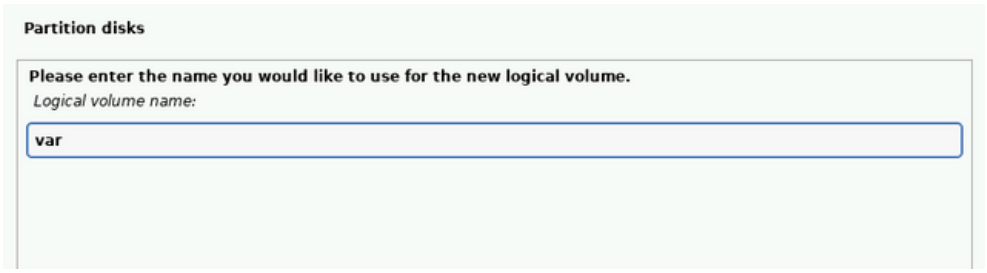
Creazione del volume logico **var**

selezioniamo **Create logical volume**

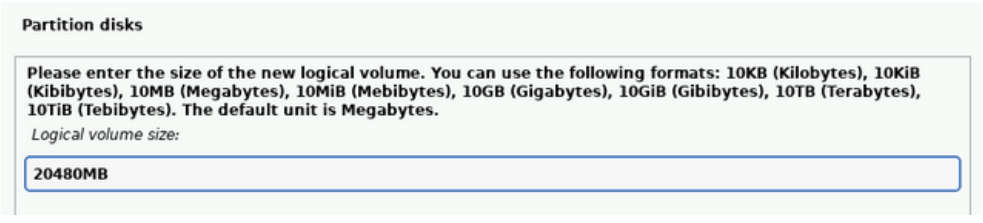
selezioniamo il **Volume Group**



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



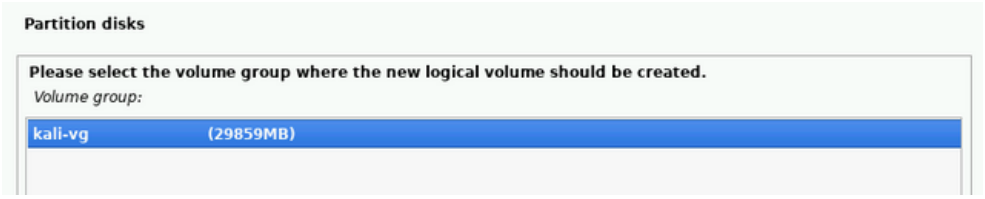
impostiamo la grandezza desiderata, **20480 MB**



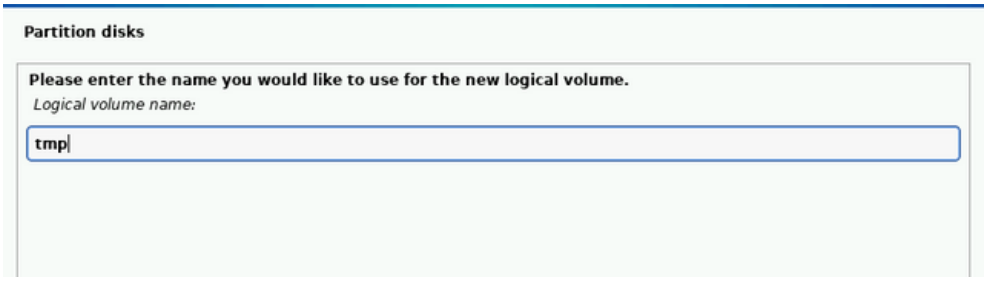
Creazione del volume logico **tmp**

selezioniamo **Create logical volume**

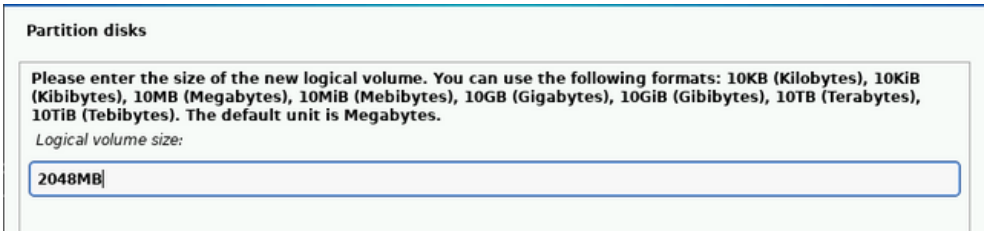
selezioniamo il **Volume Group**



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



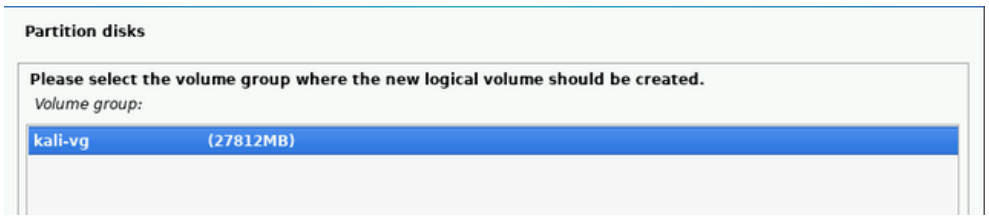
impostiamo la grandezza desiderata, **2048 MB**



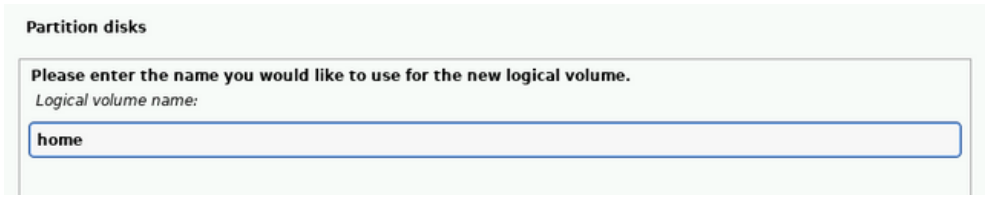
Creiamo il volume logico finale per la directory **home**

selezioniamo **Create logical volume**

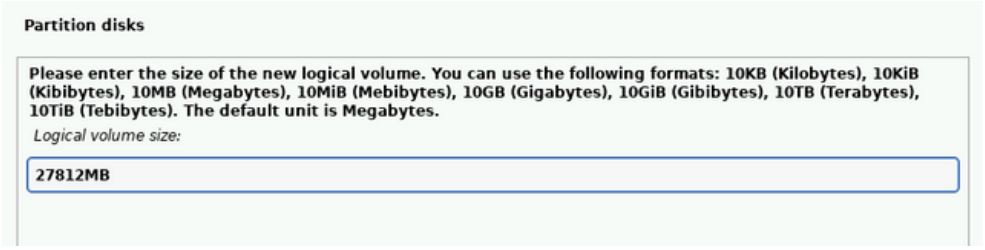
Selezioniamo nuovamente lo spazio libero nel Volume Group kali-vg,
*Assegniamo il nome **home** e dedichiamo **tutto lo spazio rimanente** a questa partizione.*



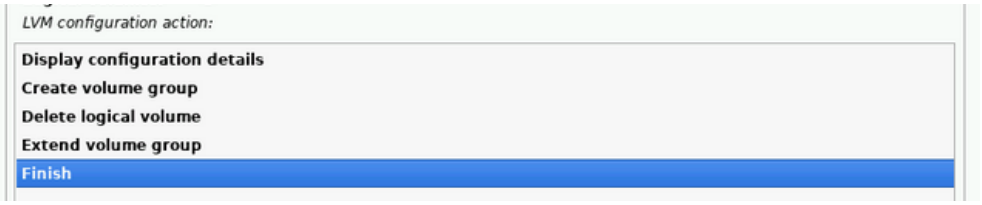
inseriamo **home**



inseriamo **la grandezza desiderata**



selezioniamo **Finish**

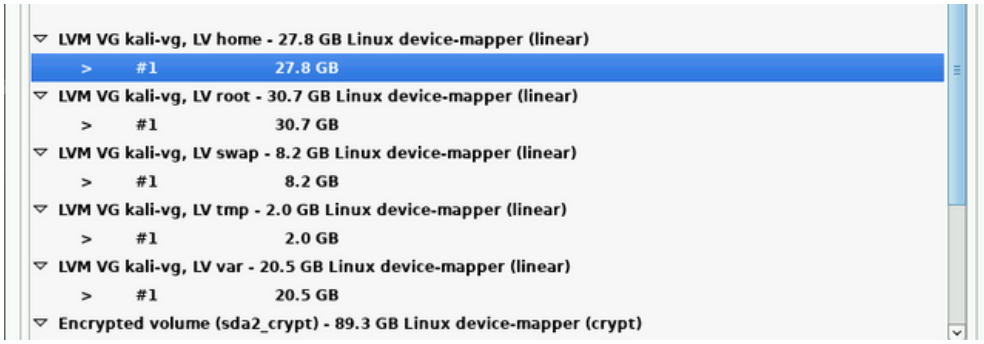


selezionare **Finish partitioning and write changes to disk**

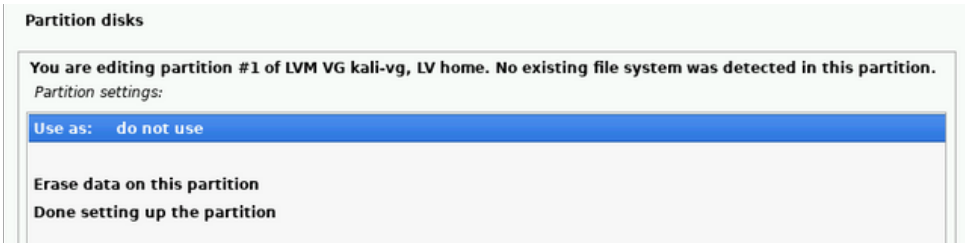
*Terminata la configurazione **LVM**, selezioniamo '**Finish**' per completare la fase di partizionamento logico e procedere alla configurazione dei **mount point** per ciascun volume.*

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

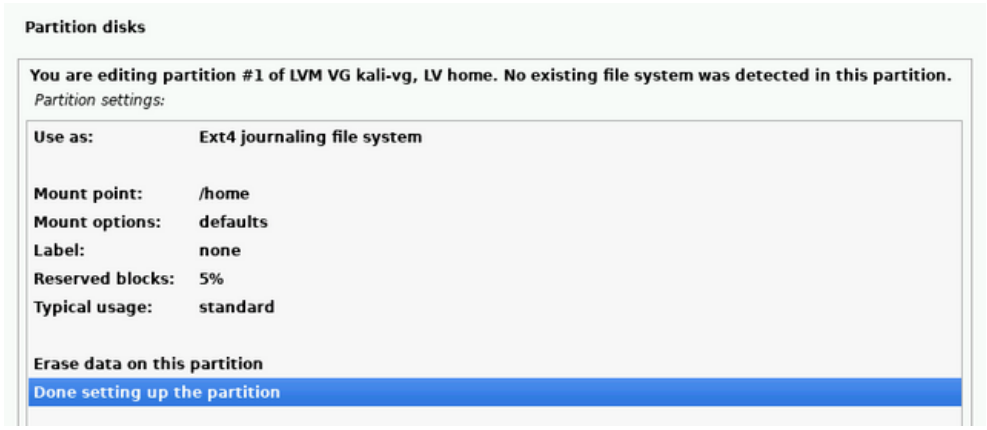
Cominciamo con **home**



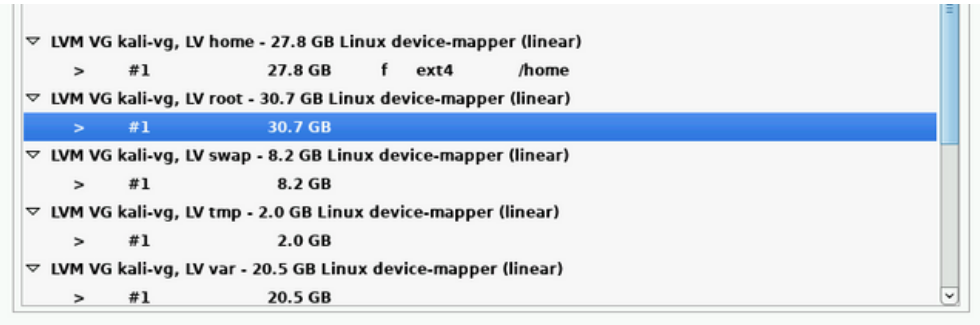
modifichiamo **Use as: do not use** in **Ext4 journaling file system**



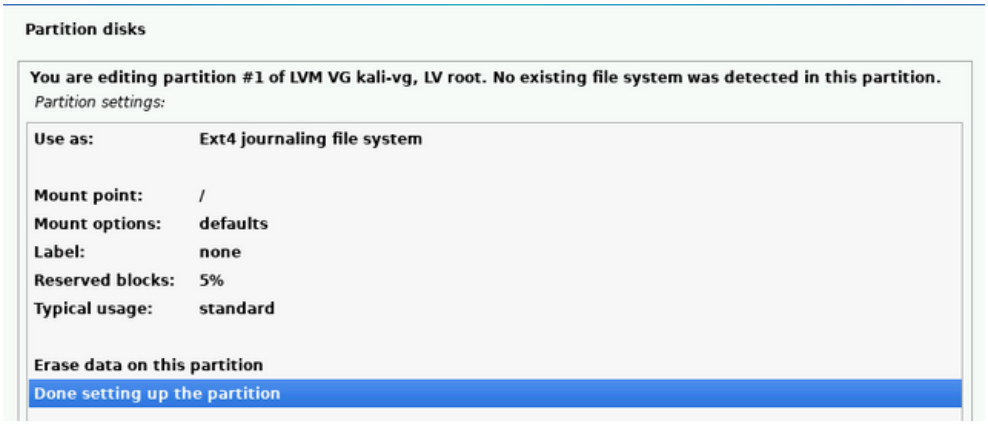
settiamo **Mount point:** a **/home**
selezioniamo **Done setting up the partition**



Impostiamo i **File System**, i **Mount Point** di **Root**



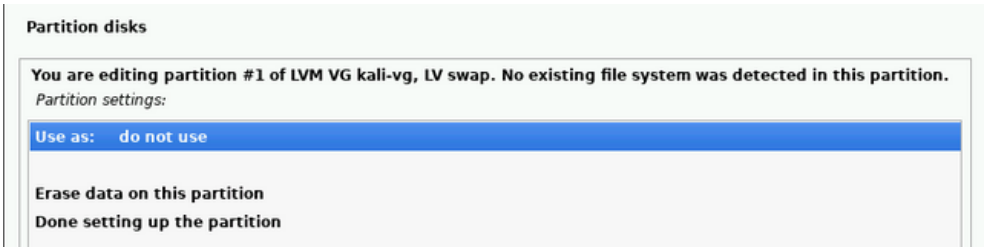
modifichiamo **Use as: do not use** in **Ext4 journaling file system**
settiamo il **Mount point** a **/ - the root file system**



selezioniamo **Done setting up the partition**

Impostiamo i **File System**, i **Mount Point** di **swap**

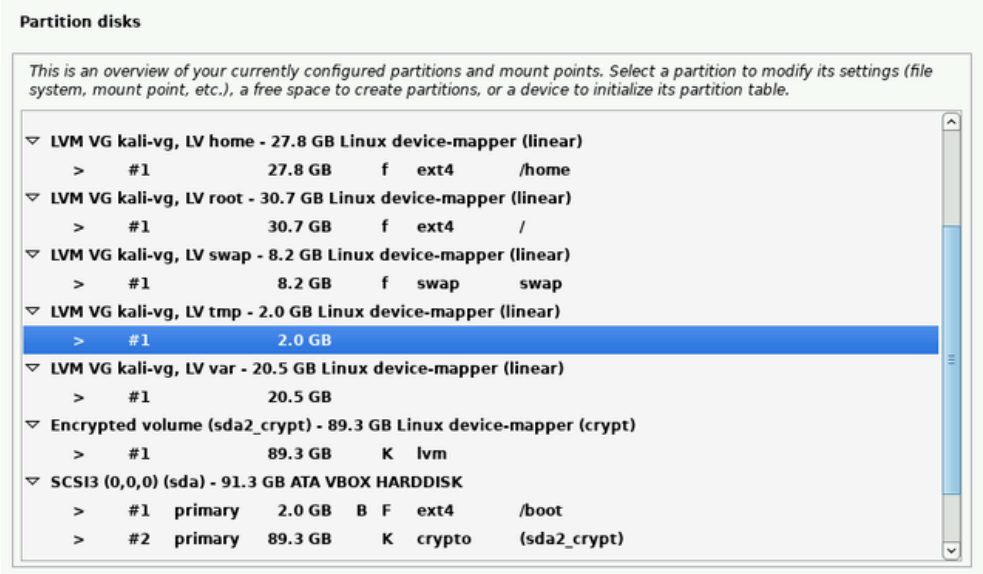
modifichiamo ***Use as: do not use***



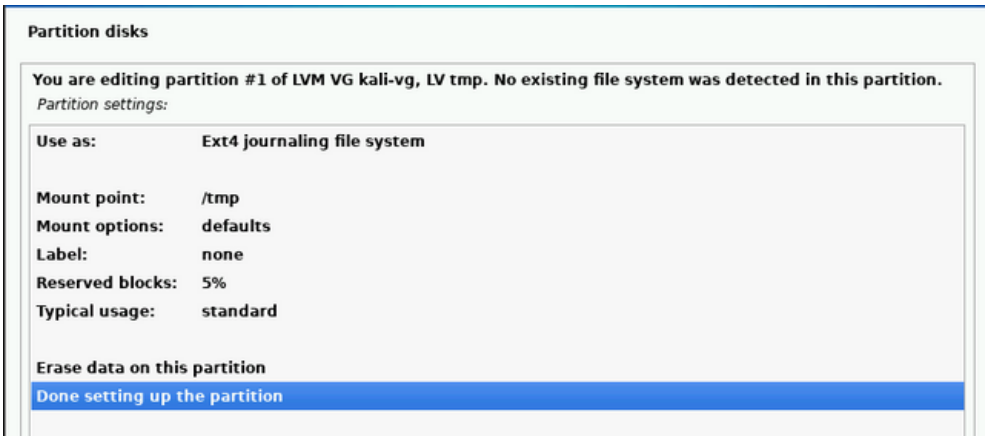
selezioniamo ***swap area***

selezioniamo **Done setting up the partition**

Impostiamo i **File System**, i **Mount Point** di **tmp**

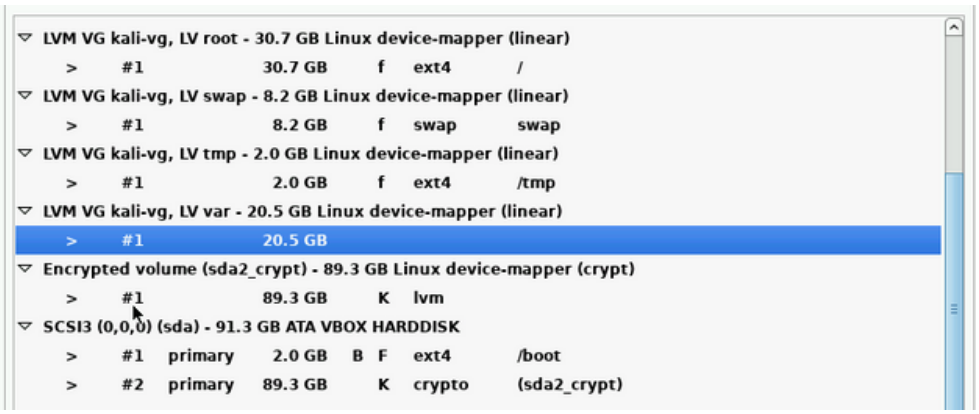


modifichiamo **Use as: do not use** in **Ext4 journaling file system**
settiamo il **Mount point** a **/temp**

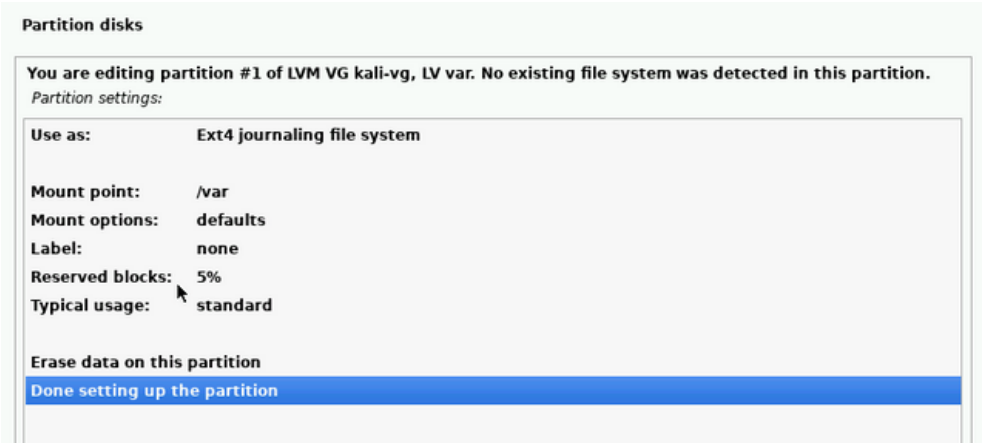


selezioniamo **Done setting up the partition**

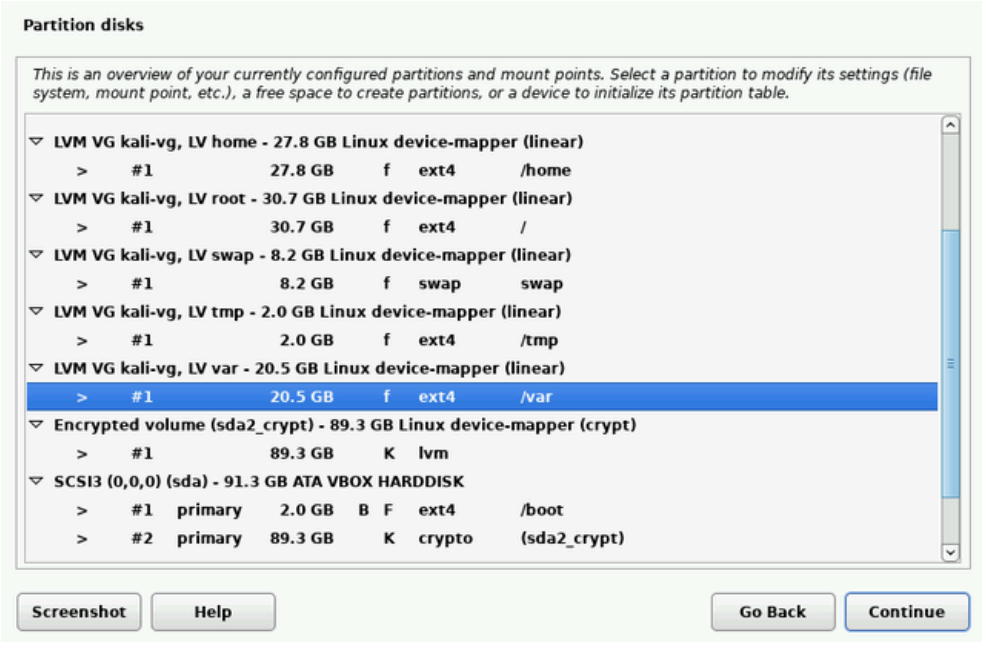
Impostiamo i **File System**, i **Mount Point** di **var**



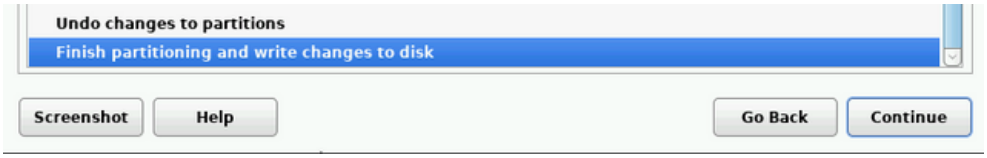
modifichiamo **Use as: do not use** in **Ext4 journaling file system**
settiamo il **Mount point** a **/var**



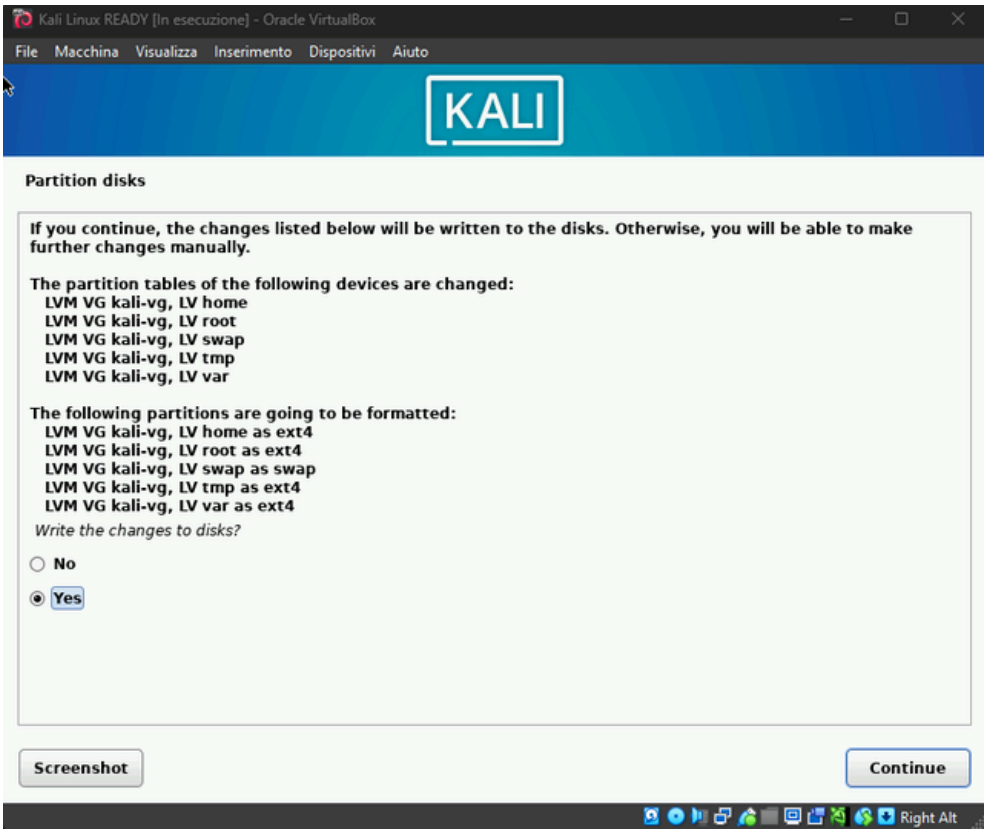
selezioniamo **Done setting up the partition**

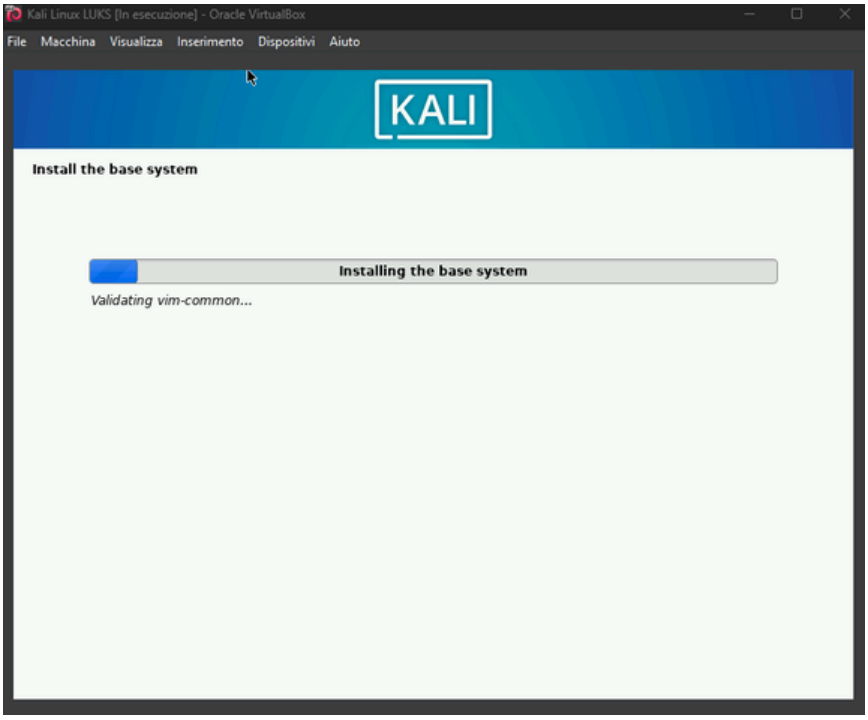


Una volta impostate le unita' logiche
selezioniamo **Finish partitioning and write changes to disk**

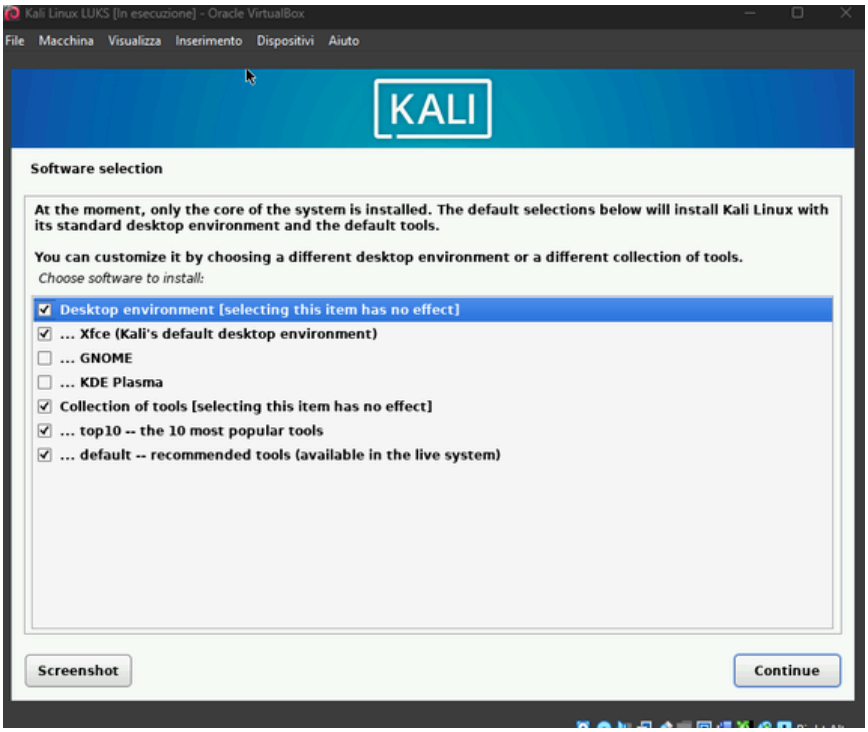


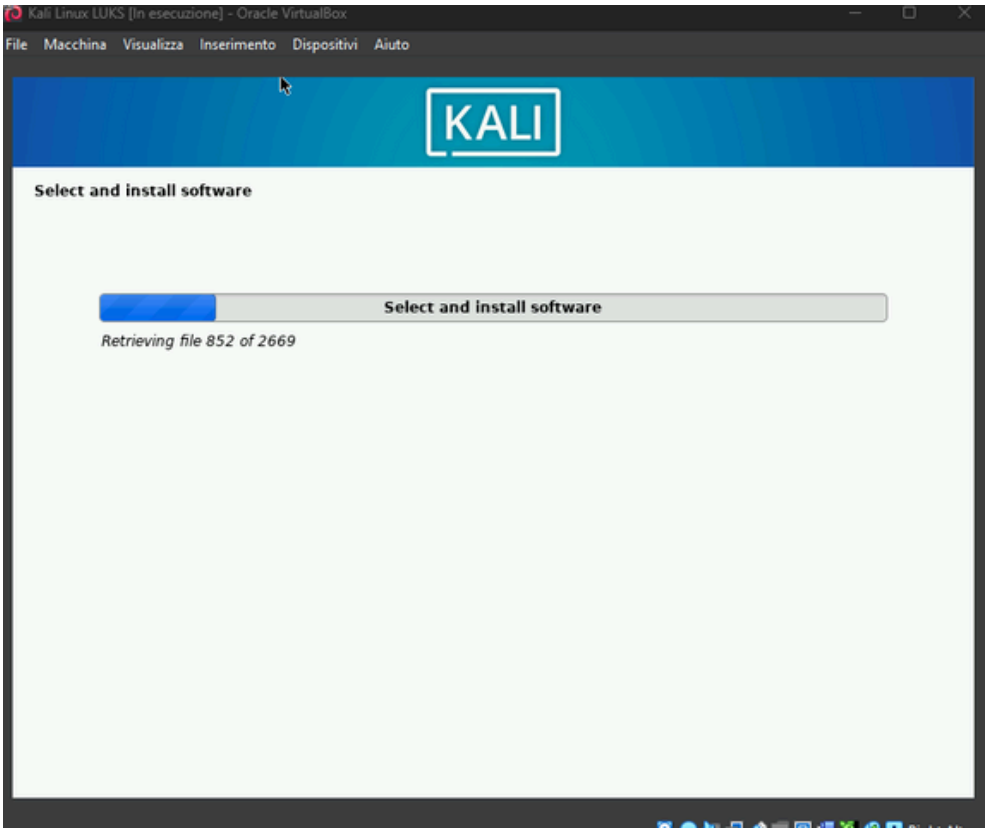
confermiamo con **YES**



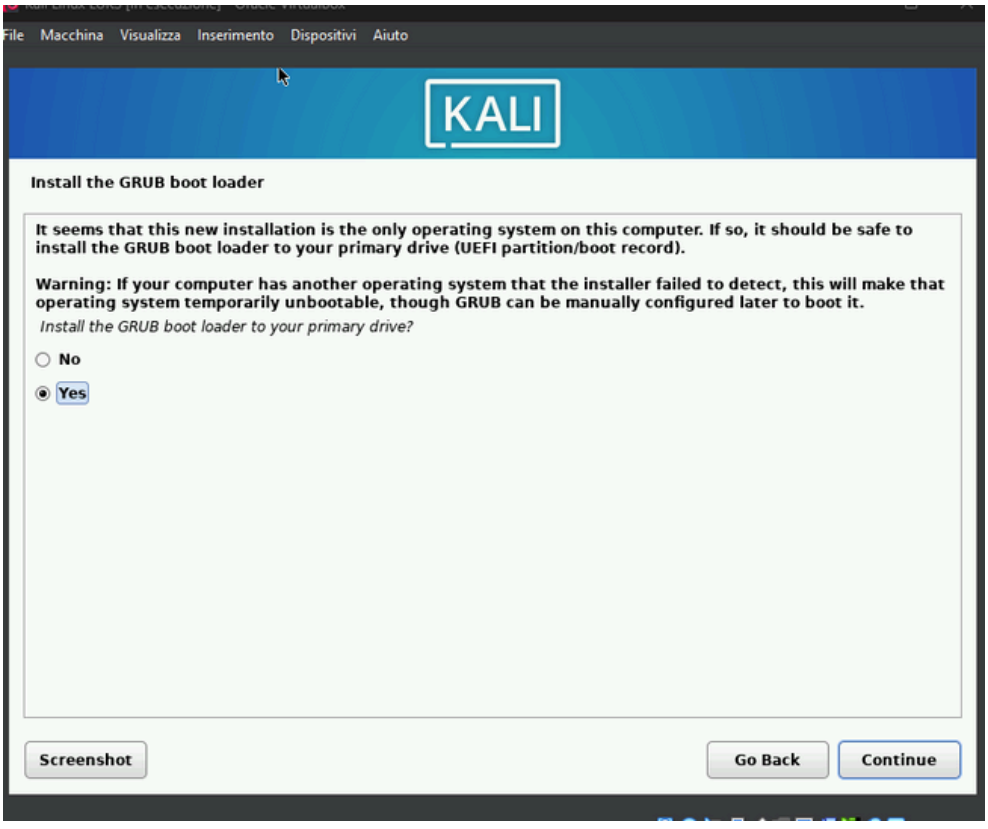


selezionare i **contenuti** da **installare**

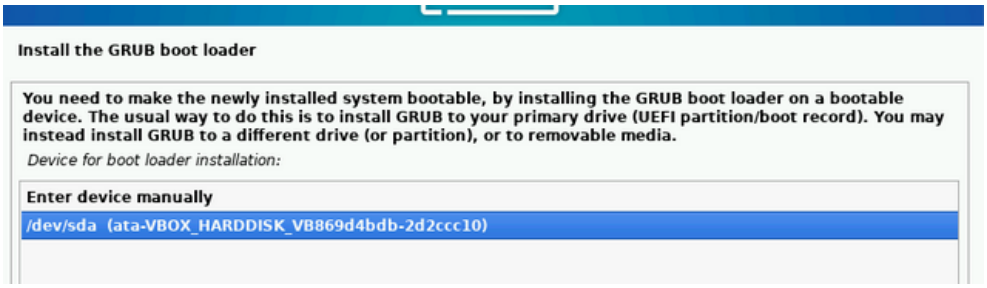




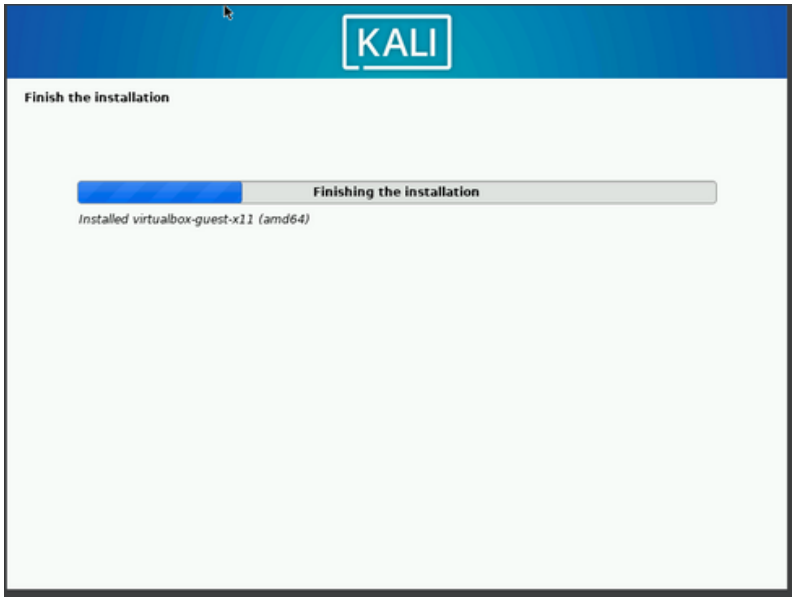
*confermiamo con **yes***



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*