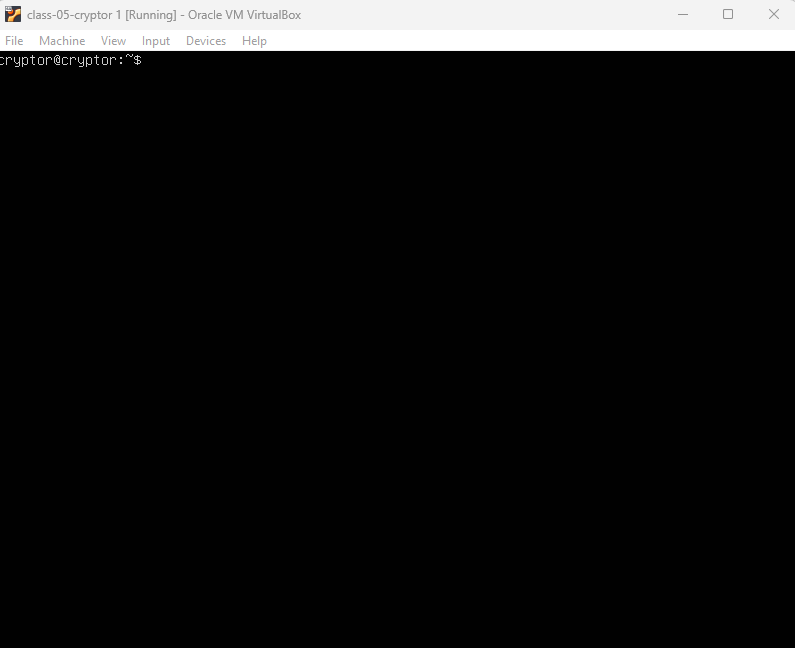
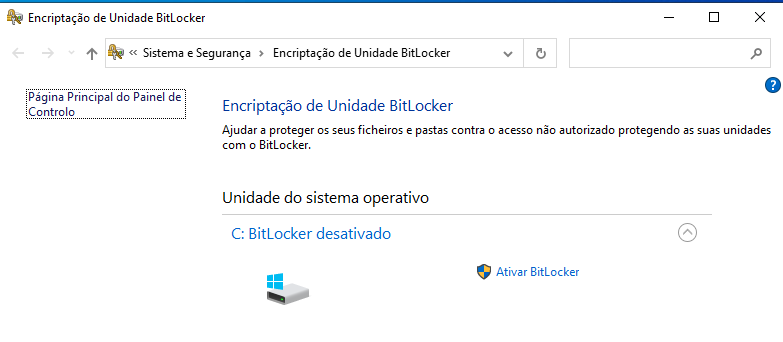
Rodrigo Brasil 11/2023

### **Part 1: Staging**

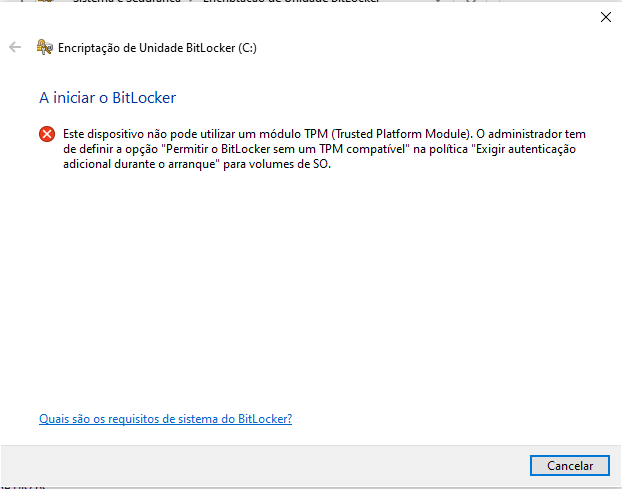
Windows 10 VM Deployed

Cryptor (Ubuntu Server) VM Deployed

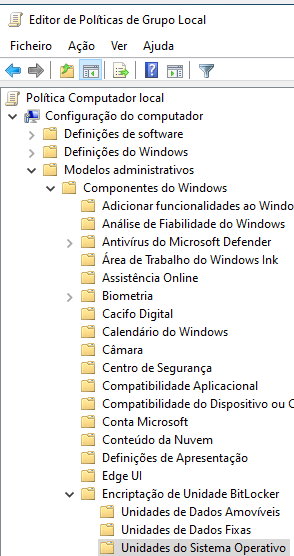
### **Part 2: Windows FDE**



Search in the windows search bar for bitlocker it will show this menu



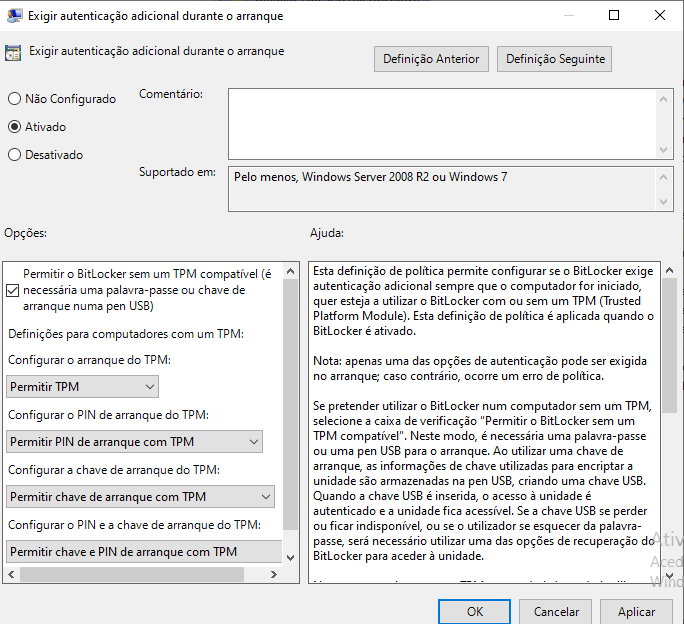
Because we are trying to encrypt a VM disk this error will show up



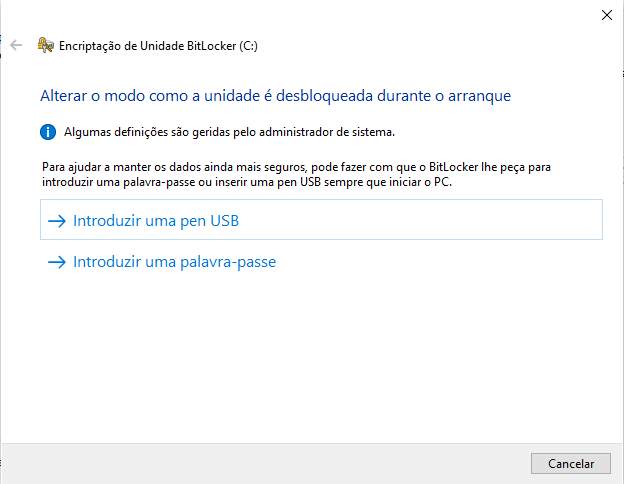
To fix this error we need to edit a local group policy by running run.exe and typing gpedit.msc.

Navigating to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives





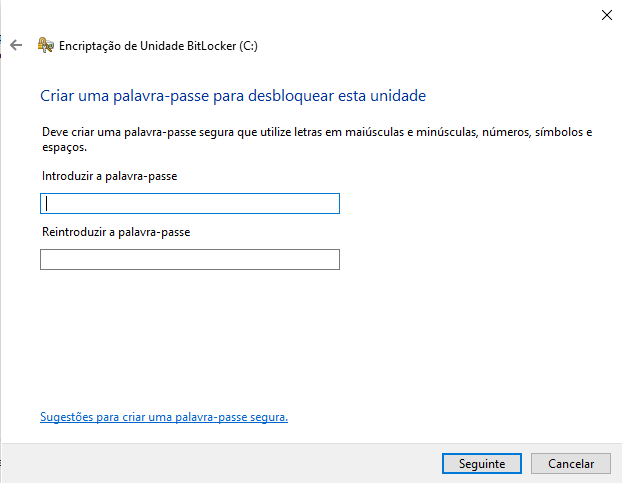
And editing the “Require additional authentication at startup” policy as it’s shown in the screenshot above



After configuring the policy we can now enable BitLocker.

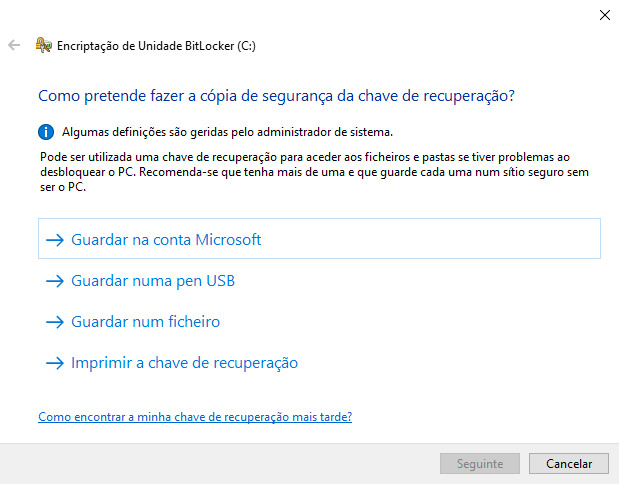
In this screenshot it is asking the method that we want to use to decrypt the disk during the OS boot.

For this exercise I'm going to choose a password.



After choosing the password option it is going to ask for a password

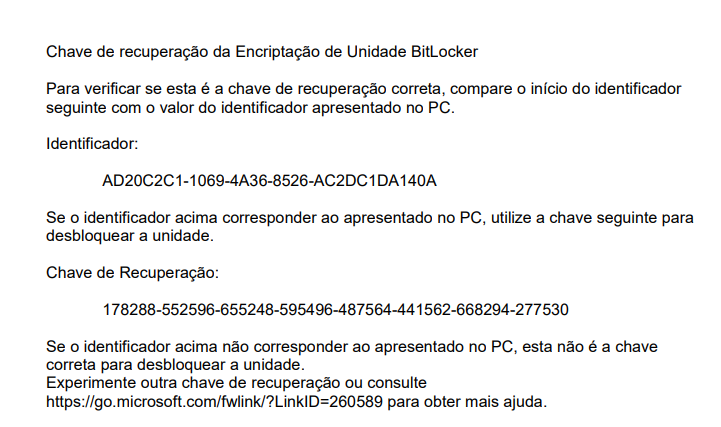
For this exercise the password is going to be Password1!



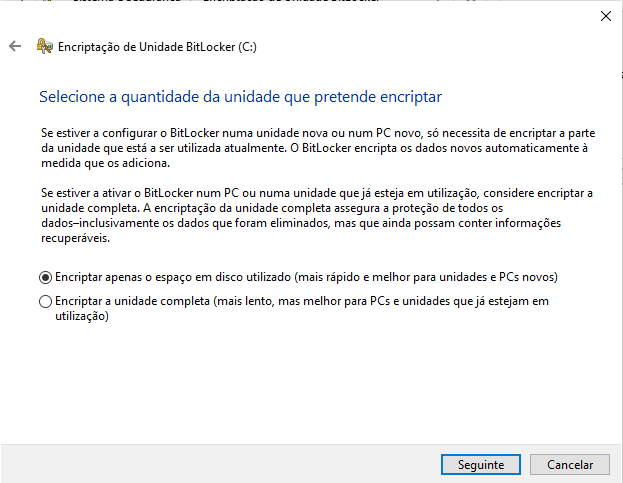
After introducing the password it will ask how we want to store the recovery key

we will select print, save it in pdf and save it on the local machine

of course in a real world scenario we want to save the key somewhere else like a server

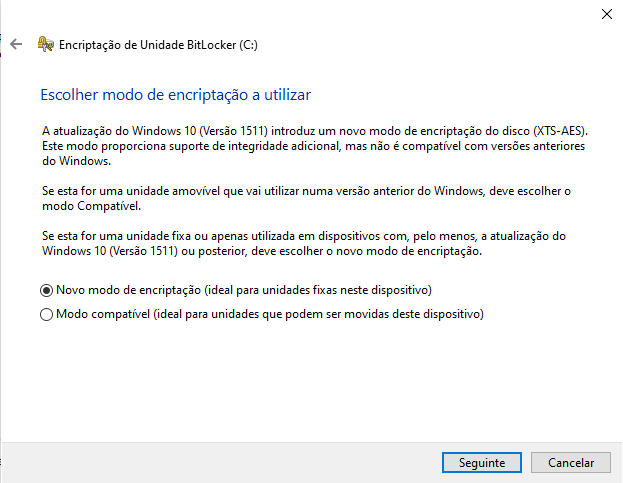


Windows 10 VM BitLocker Recovery key



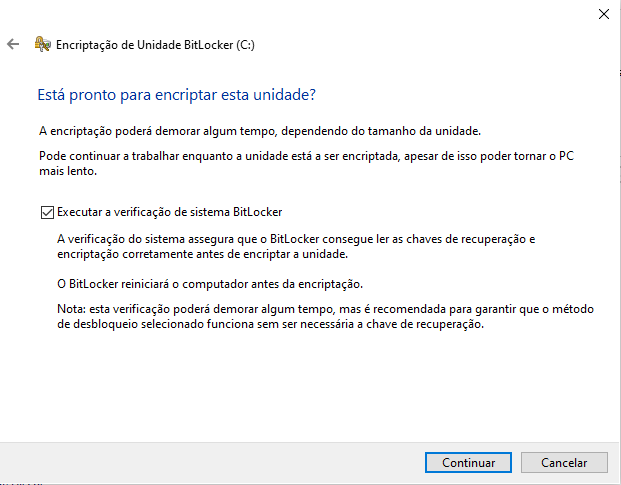
in this step it will ask if we want to encrypt only a bit of space on the hard drive or the whole drive

for this exercise we are going to encrypt the whole drive

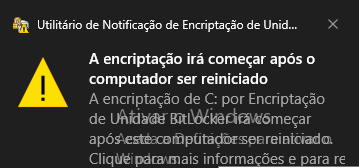


In this step it will ask what mode of encryption we want, new encryption mode or compatibility mode. New encryption mode is for fixed storage drives and compatibility mode is for external storage drives.

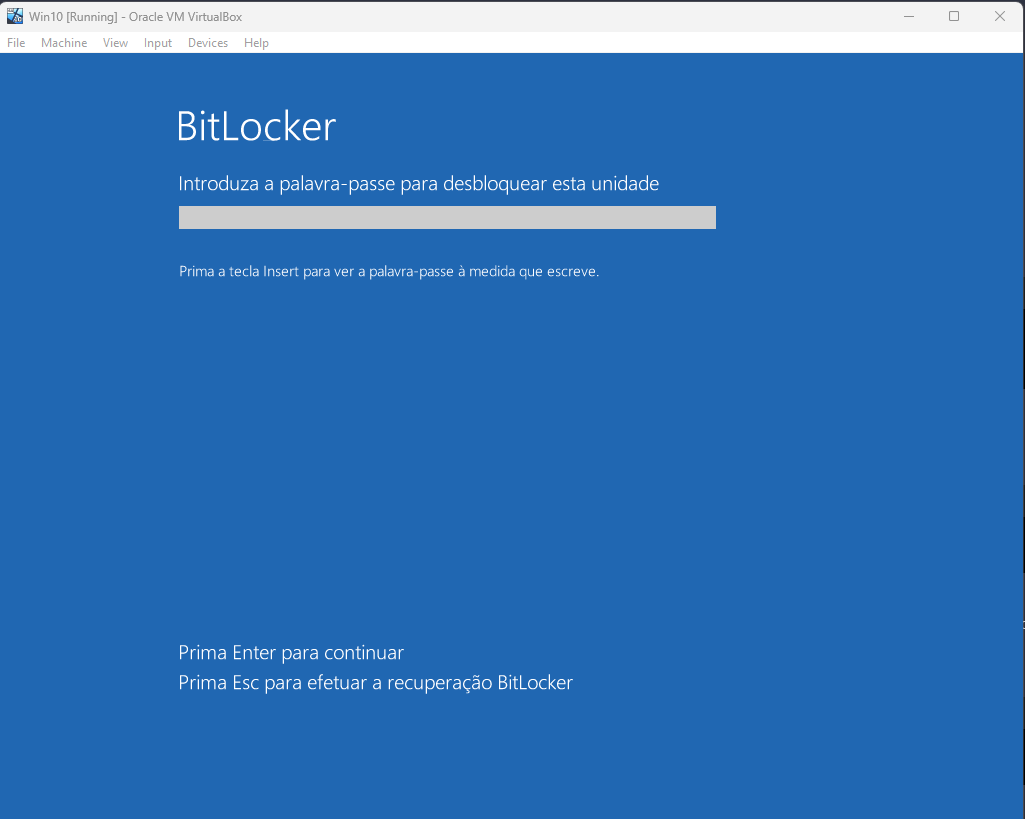
For this exercise we are going to select “new encryption mode” for obvious reasons.



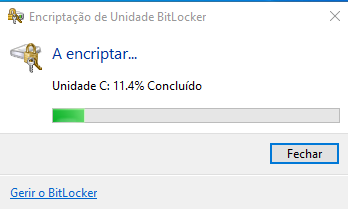
In this step just make sure the checkbox is checked so BitLocker makes sure that it can read the Recovery key correctly

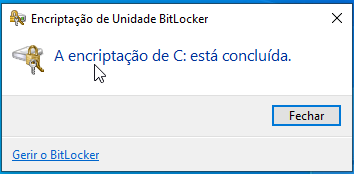


after finishing the configuration this notification will pop up saying the encryption will start after rebooting the machine



After rebooting it will ask for the password that was made in a inicial step





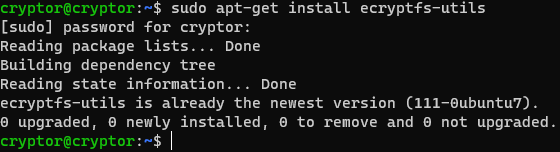
After rebooting BitLocker will start encrypting the disk, now just wait until completion

### **Part 3: Linux Directory Encryption**

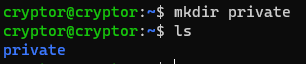


Successful ssh connection to the Cryptor (Ubuntu) VM

In this machine we will create a new directory, encrypt it and make its encrypted files readable only when mounted.



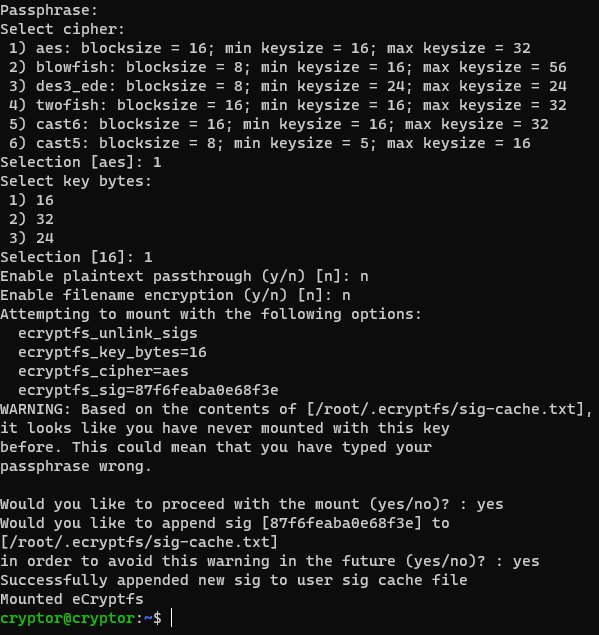
First we will check if the ecryptfs package is installed which in this case it is.



Next we will create a new directory, for this exercise we will call it private



After creating the directory we will mount it in /mnt using the encryptfs package



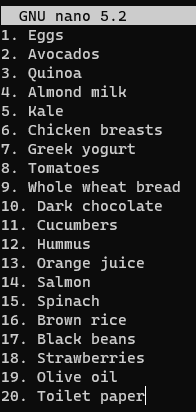
and it will ask for a passphrase, for now it will be Password1, it will ask to select a cipher for this exercise we will chose AES and for key bytes we will chose 16 for now.

it will also ask if we want to enable plaintext passthrough and filename encryption, because we want to encrypt the text inside the data file we will type n and we also don't want to encrypt the name of the file so we will also type n.

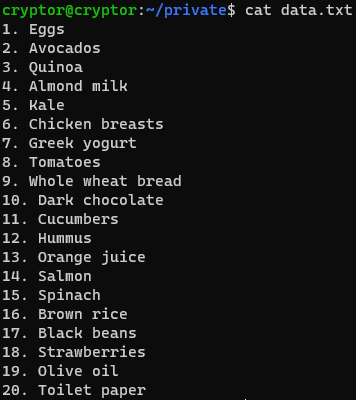


After that we will create a new text document inside the private directory, for this exercise we will call it data.





Using nano we will give the data.txt file a random shopping list



Now because we are mounted we can see the contents of the data.txt file in plain text using the cat command



but if we dismount the private directory with the umount command



and try to use the cat command on the data.txt file it will the shopping list is encrypted and will only show a ciphertext

### 

### **Part 4: Reporting**

* What is the purpose of the TPM chip and why is it normally required in order to operate BitLocker on a Windows 10 PC?
  + The purpose of the TPM chip is for key storage, cryptographic operations, and security-related tasks. It's normally required to operate BitLocker because BitLocker stores its encryption keys on the TPM chip.
* Are laptop computers secured against theft out of the box? What precautions can be taken to ensure data confidentiality in the event of laptop theft?
  + No, laptops don't come secured against theft out of the box. Some precautions would be first to have a backup of the data inside of the laptop, have full disk encryption with a strong password and if possible have enabled remote wipe.
* What data theft scenarios do today’s tools *not* defend against?
  + Tools can only do so much, data theft scenarios can be insider threats, social engineering, physical breaches and human error.
* Consider data at rest VS data in motion. How do these two categories affect how you approach securing data?
  + Securing data at rest involves measures to protect stored data, while securing data in motion focuses on safeguarding data as it travels across networks. I would have to address both states by combining encryption, access controls, network security, and monitoring to mitigate risks associated with the data storage and transmission.