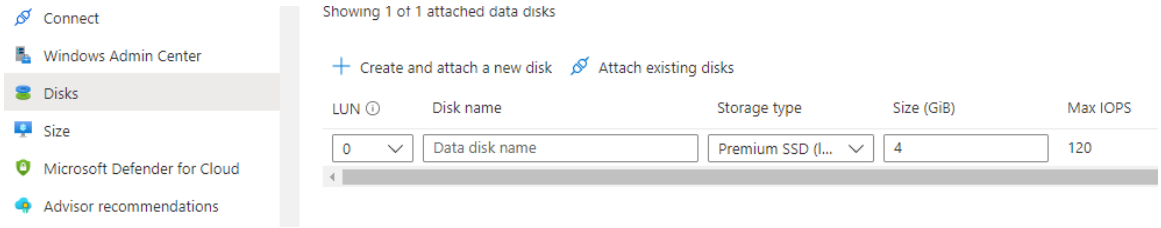
1) Create data disk
2) Attach disk to vm .

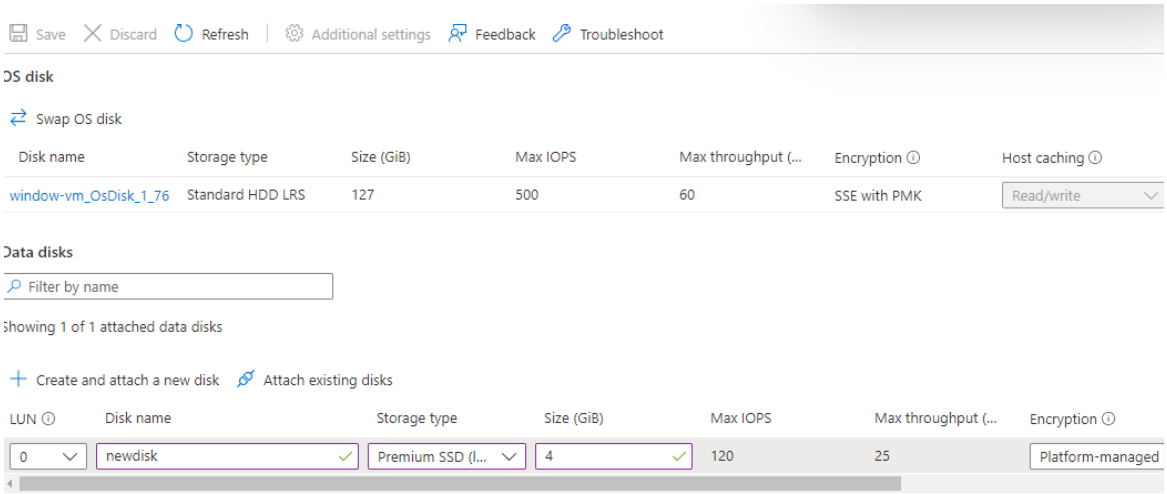
Disk is a separate resource we can attach to any vm . We can detach the disk and attach to another vm .

ADDING DISK FOR WINDOWS SERVER :



CREATE AND ATTACH NEW DISK TO VM >

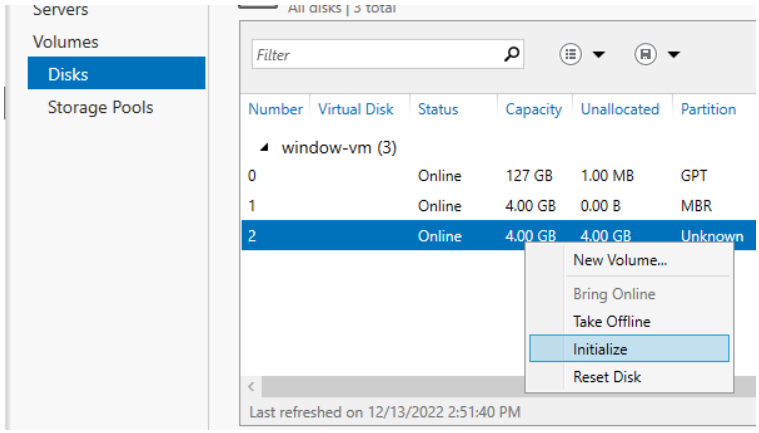
Disk name > LUN (logical unit number) > attach disk to vm > 8gb > 120iops>

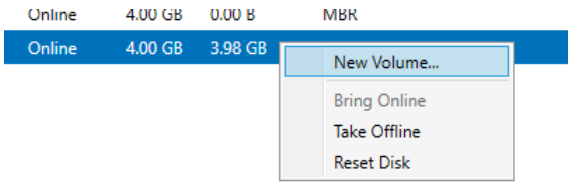


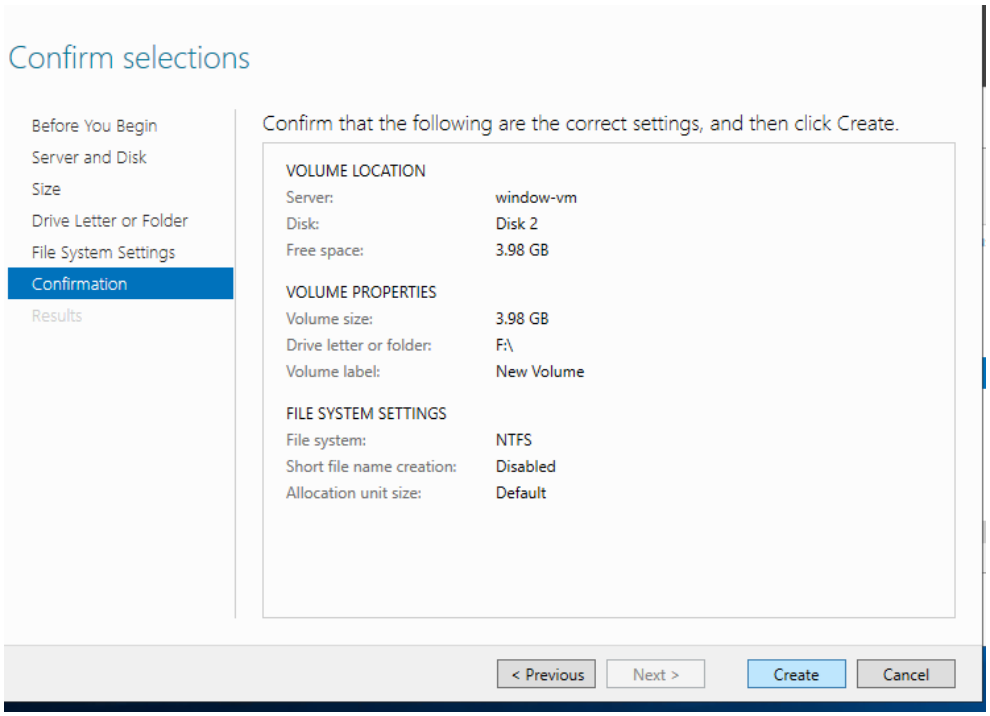
Now the disk is added to azure level .

We will add the disk to OS level now .

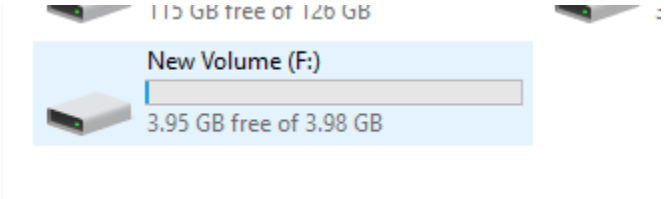
In windows server > server manager > file and storage service > Disks > DISK had unknown partition (initialize disk) > New volume > give name for volume > create >







Disk will be added to windows vm .



DIsk will be visible .

Azure managed disk - managed by azure , virtualized , high available , support features .
Disk type - standard hdd , standard sdd , premium sdd .

SERVER SIDE DISK ENCRYPTION :

When it comes to this security feature, this is disk encryption via virtual machines. Now, your data disk might be containing some crucial information, some sensitive information, and this data will be stored in a data center.
Now most organizations still have this requirement that even though the data is being hosted in a data center, it needs to be encrypted at rest.

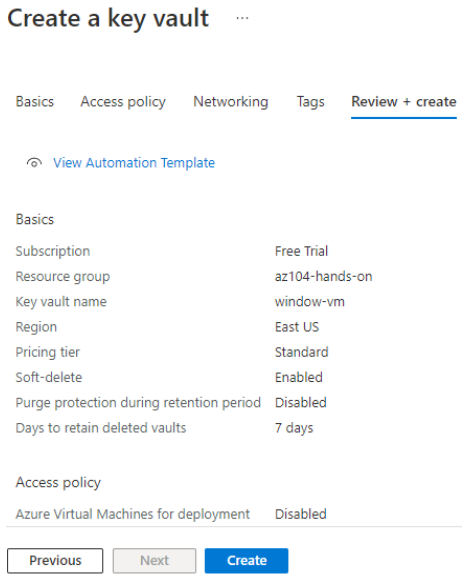
This means that when the data is finally stored on the disk in your data center on these physical disks, it needs to be encrypted.
This is so that even if the disk where to get into the wrong hands, the malicious user would not be able to get that information without being able to decrypt the information fast.
So there is a security feature known as server side disk encryption, which ensures that the data on the disk are encrypted at rest.
So this is available for the most disk, and it's available for both your OS level disk and your data disk. aswell.
Your data is automatically encrypted,

When it comes to encryption, it is server side encryption. PMG means the platform manager keys.
The same goes for the data disk as well. When you want to encrypt data, you need to use an encryption key along with an algorithm for encrypting the data.
You know, the keys are being managed by the azure platform themselves.
You also have the ability to also use customer managed keys.
Sometimes organizations want to ensure that they manage the encryption keys.

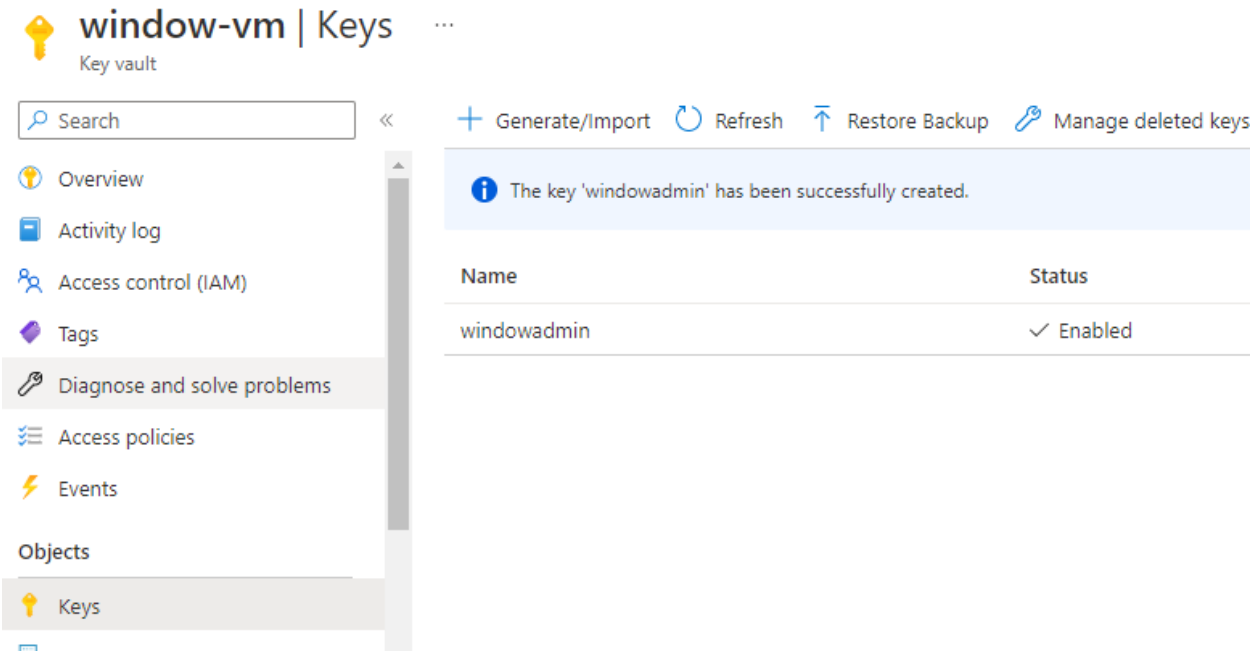
CUSTOMER MANAGED KEY

We can add a customer encryption key . We use an azure key vault - managed service to store encryption keys .

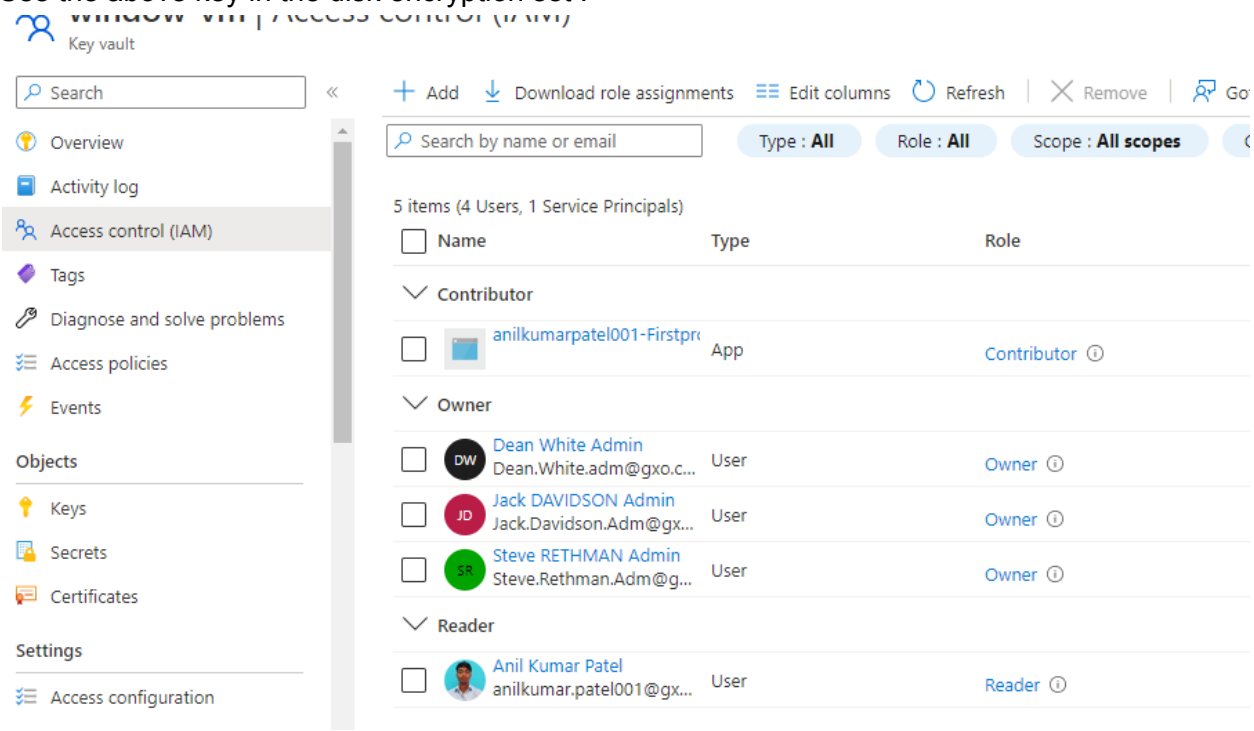
Create key vault service .> days to retain 7 days > create key vault > create key .



Create a key in the key vault .

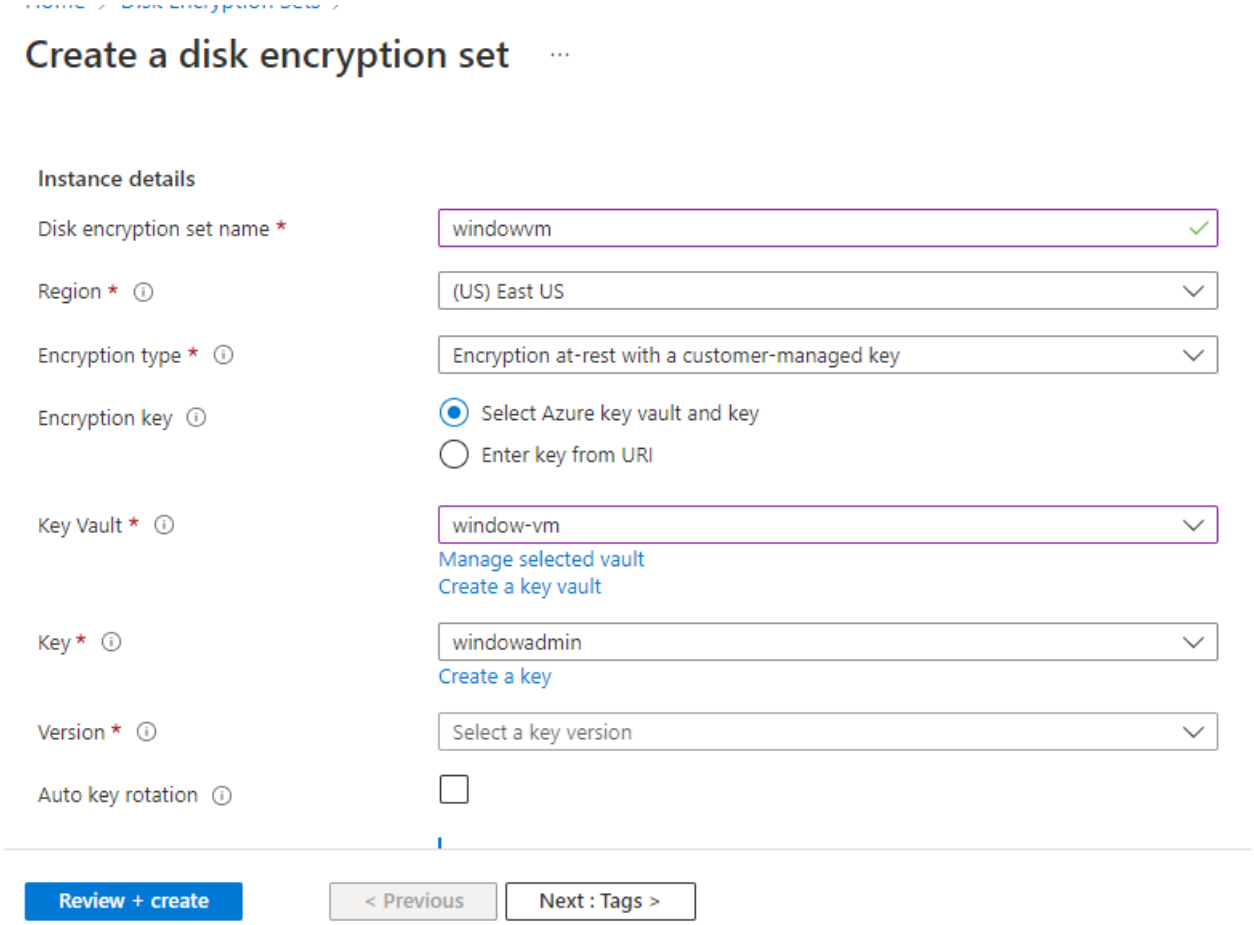


Use the above key in the disk encryption set .

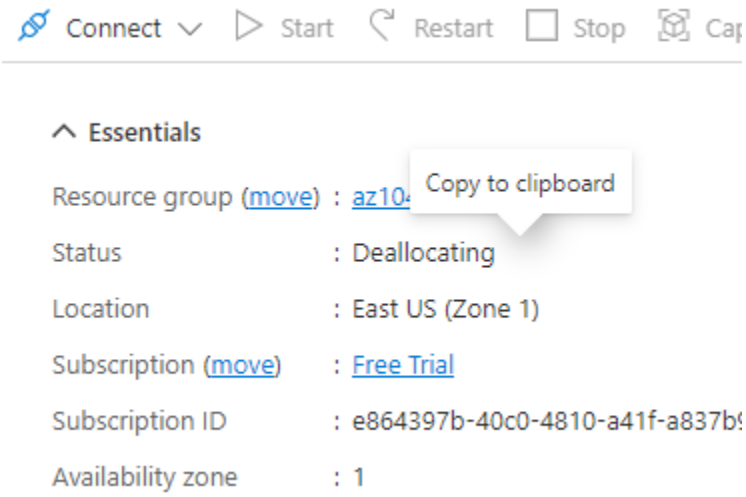


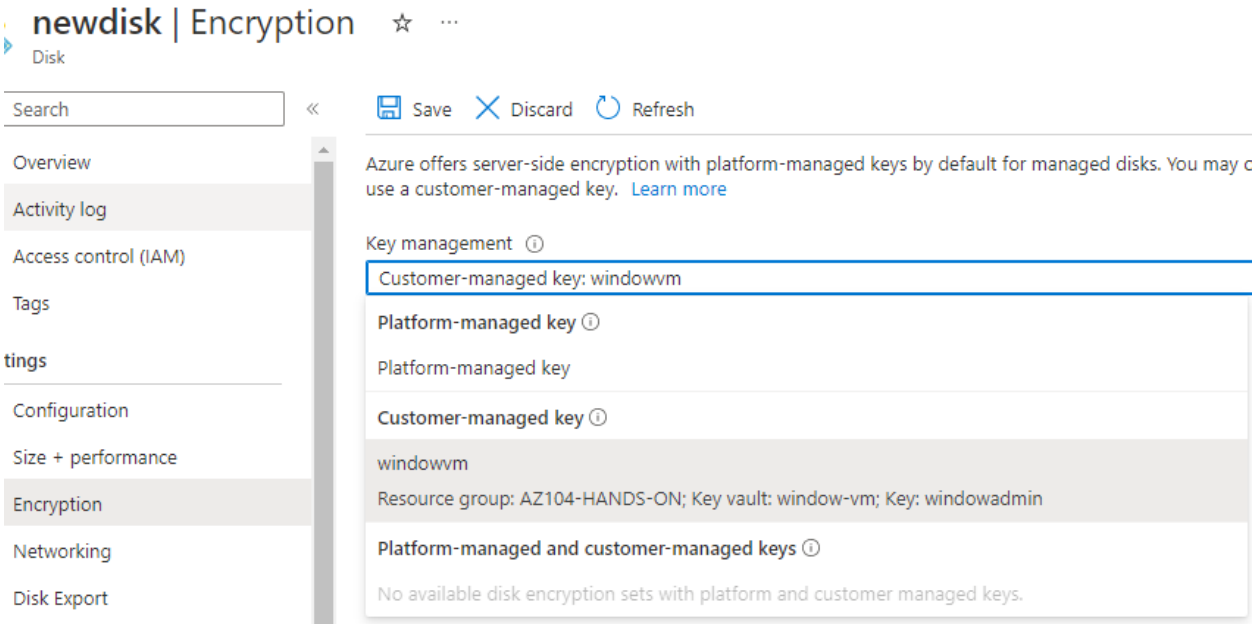
Assign the reader role to your account . - if you don't assign the reader role then you will get an error .

Create disk encryption key set> Create > select created key > create >



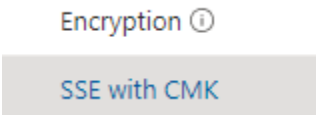
To use customer managed keys , we have to stop vm . Go to disk > encryption > select disk encryption set .
Stop vm





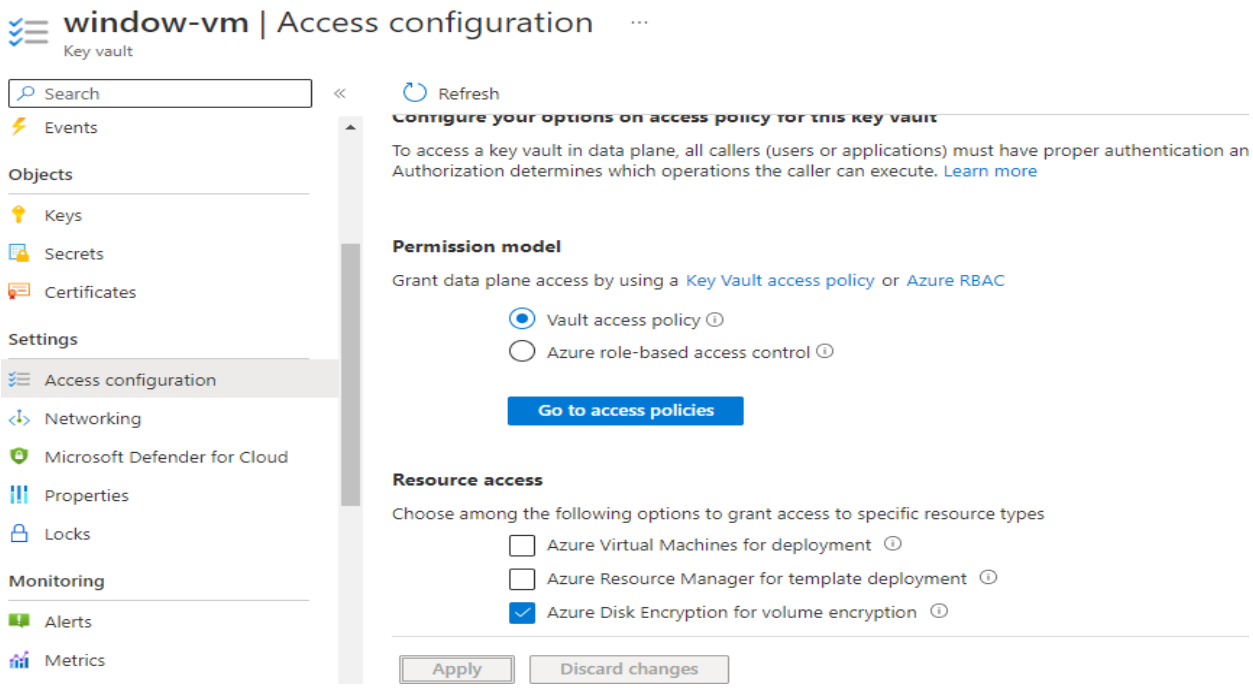
Change encryption key .

Now the encryption key for the disk is updated to the customer encryption key .

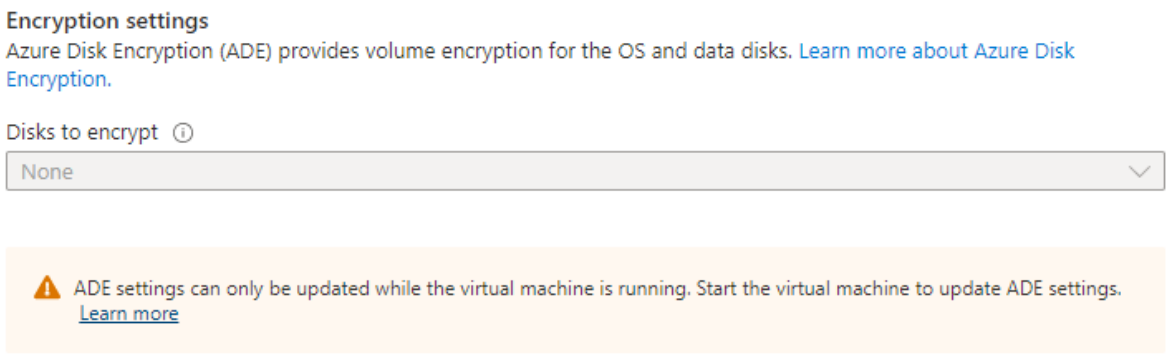


ENABLE AZURE DISK ENCRYPTION FOR DISK :

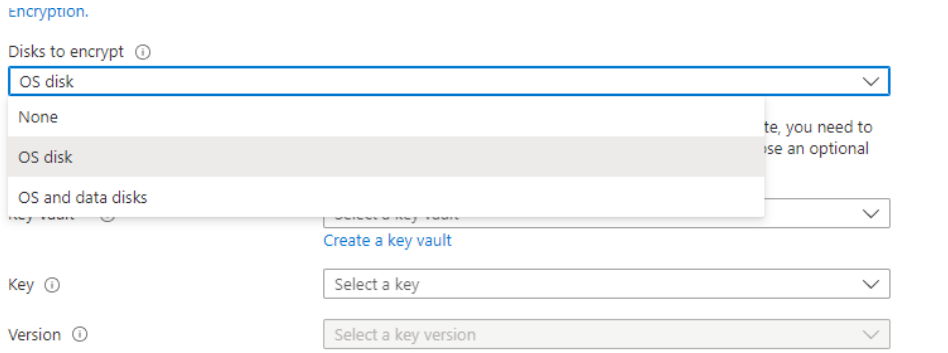
We need an azure key vault in the same location as vm .
In key vault > access configuration > enable azure disk encryption for volume encryption .
Create key >



Go to vm > DISK > Additional setting > We can enable disk encryption .



We need to start vm to enable ade .



We can select the disk to enable ade .