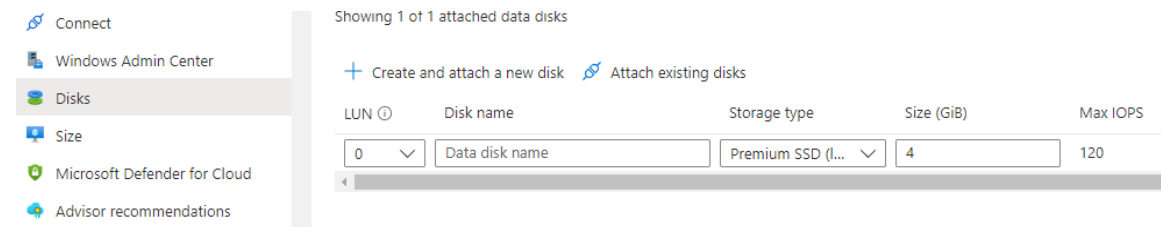


- 1) Create data disk
- 2) Attach disk to vm .

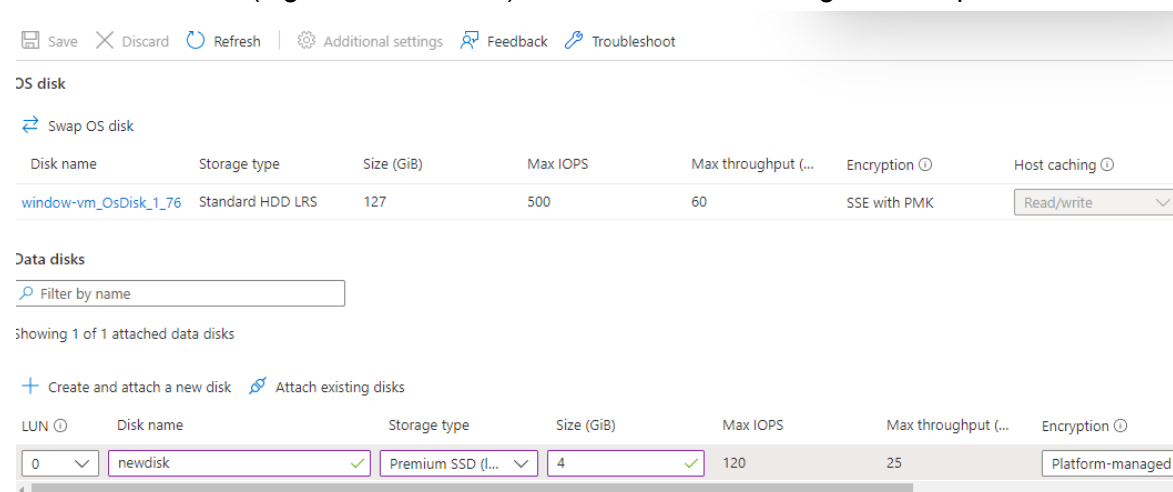
Disk is a separate resource we can attach to any vm . We can detach the disk and attach to another vm .

ADDING DISK FOR WINDOWS SERVER :



CREATE AND ATTACH NEW DISK TO VM >

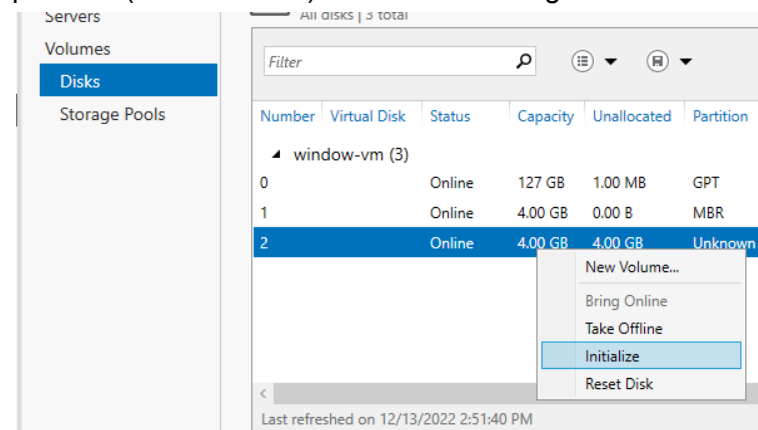
Disk name > LUN (logical unit number) > attach disk to vm > 8gb > 120iops>

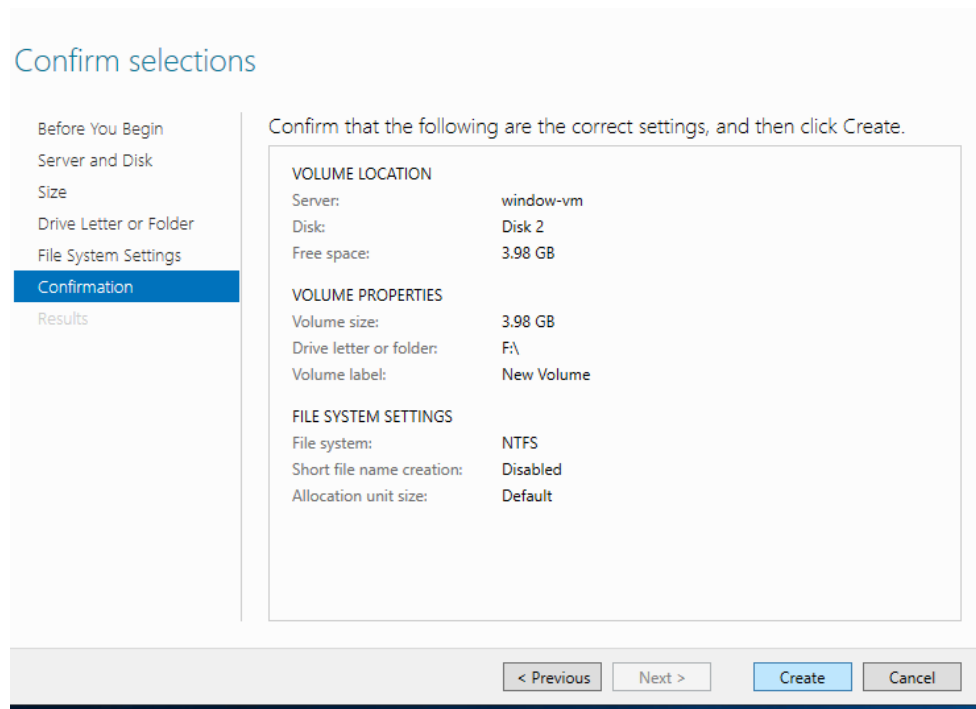
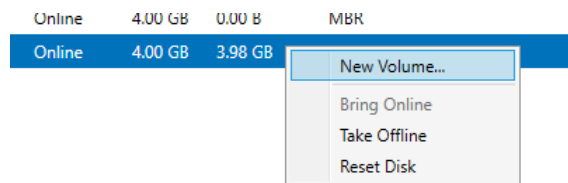


Now the disk is added to azure level .

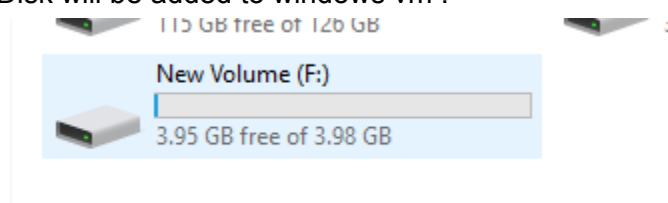
We will add the disk to OS level now .

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 were 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 vault ...

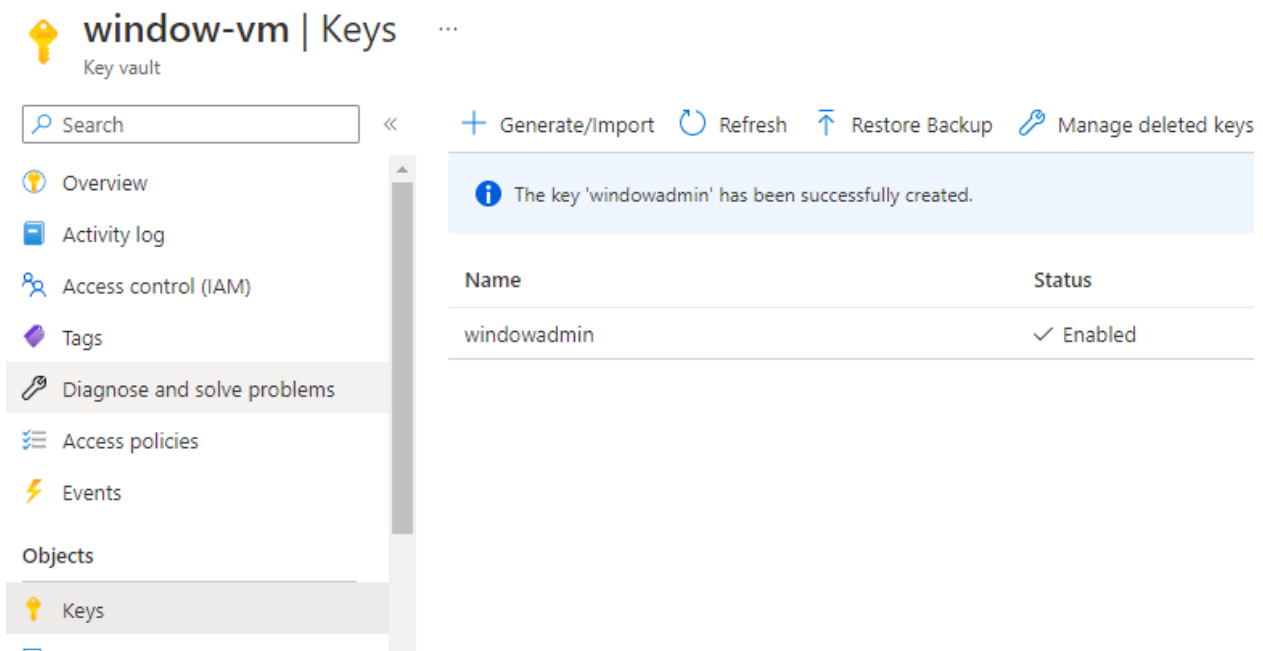
The screenshot shows the 'Review + create' step of the 'Create a key vault' wizard in the Azure portal. The interface includes a progress bar at the top with tabs for 'Basics', 'Access policy', 'Networking', 'Tags', and 'Review + create'. Below the progress bar is a link to 'View Automation Template'. The main content area is divided into two sections: 'Basics' and 'Access policy'. The 'Basics' section contains a table of configuration details. The 'Access policy' section shows 'Azure Virtual Machines for deployment' set to 'Disabled'. At the bottom, there are three buttons: 'Previous', 'Next', and 'Create'.

Basics	
Subscription	Free Trial
Resource group	az104-hands-on
Key vault name	window-vm
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	7 days

Access policy	
Azure Virtual Machines for deployment	Disabled

Previous Next Create

Create a key in the key vault .



Key vault

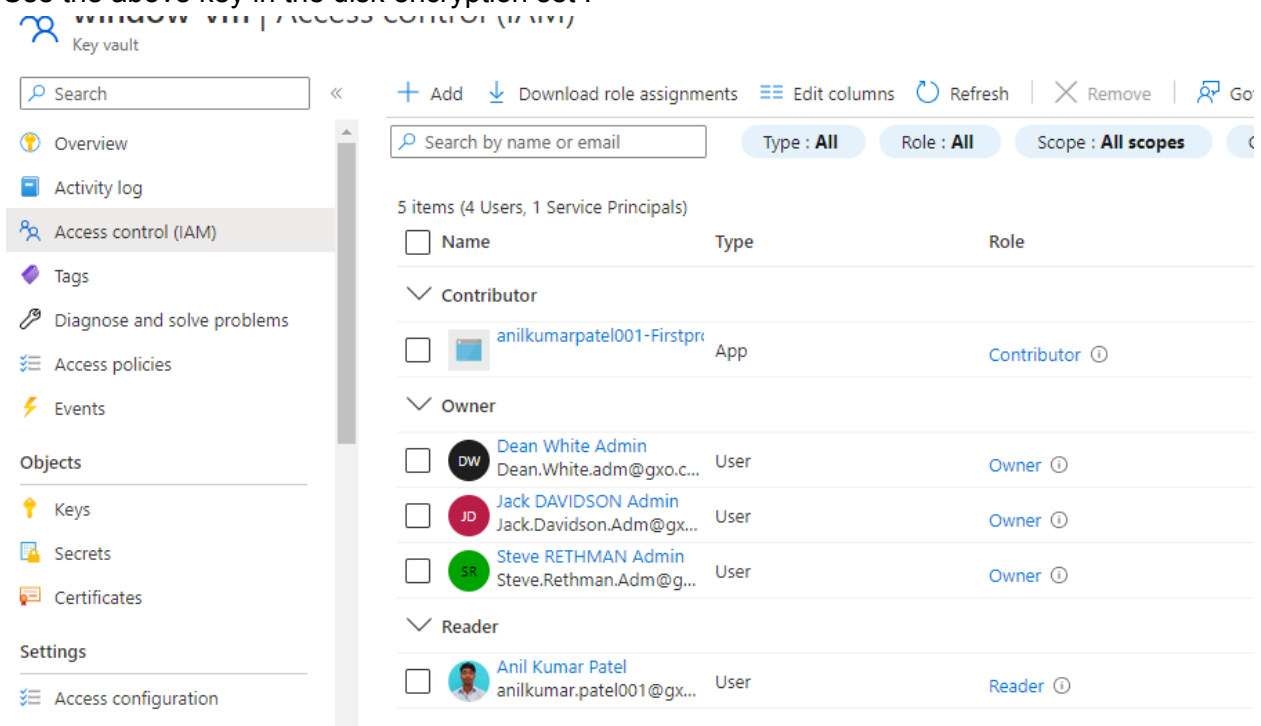
Search

Generate/Import Refresh Restore Backup Manage deleted keys

The key 'windowadmin' has been successfully created.

Name	Status
windowadmin	✓ Enabled

Use the above key in the disk encryption set .



Key vault

Search

Add Download role assignments Edit columns Refresh Remove Go

Search by name or email Type: All Role: All Scope: All scopes

5 items (4 Users, 1 Service Principals)

Name	Type	Role
Contributor		
<input type="checkbox"/> anilkumarpatel001-Firstpr	App	Contributor ⓘ
Owner		
<input type="checkbox"/> Dean White Admin Dean.White.adm@gxo.c...	User	Owner ⓘ
<input type="checkbox"/> Jack DAVIDSON Admin Jack.Davidson.Adm@gx...	User	Owner ⓘ
<input type="checkbox"/> Steve RETHMAN Admin Steve.Rethman.Adm@g...	User	Owner ⓘ
Reader		
<input type="checkbox"/> Anil Kumar Patel anilkumar.patel001@gx...	User	Reader ⓘ

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 >

Create a disk encryption set ...

Instance details

Disk encryption set name *

windowvm ✓

Region * ⓘ

(US) East US ▼

Encryption type * ⓘ

Encryption at-rest with a customer-managed key ▼

Encryption key ⓘ

☒ Select Azure key vault and key
☐ Enter key from URI

Key Vault * ⓘ

window-vm ▼
[Manage selected vault](#)
[Create a key vault](#)

Key * ⓘ

windowadmin ▼
[Create a key](#)

Version * ⓘ

Select a key version ▼

Auto key rotation ⓘ

☐

Review + create

< Previous

Next : Tags >

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

 Connect ▼  Start  Restart ☐ Stop  Cap

^ Essentials

Resource group (move) : az10

Copy to clipboard

Status : Deallocating

Location : East US (Zone 1)

Subscription (move) : [Free Trial](#)

Subscription ID : e864397b-40c0-4810-a41f-a837b9

Availability zone : 1

newdisk | Encryption

Disk

Search

Overview

Activity log

Access control (IAM)

Tags

tings

Configuration

Size + performance

Encryption

Networking

Disk Export

Save

Discard

Refresh

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may c use a customer-managed key. [Learn more](#)

Key management ⓘ

Customer-managed key: windowvm

Platform-managed key ⓘ

Platform-managed key

Customer-managed key ⓘ

windowvm

Resource group: AZ104-HANDS-ON; Key vault: window-vm; Key: windowadmin

Platform-managed and customer-managed keys ⓘ

No available disk encryption sets with platform and customer managed keys.

Change encryption key .

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

Encryption ⓘ

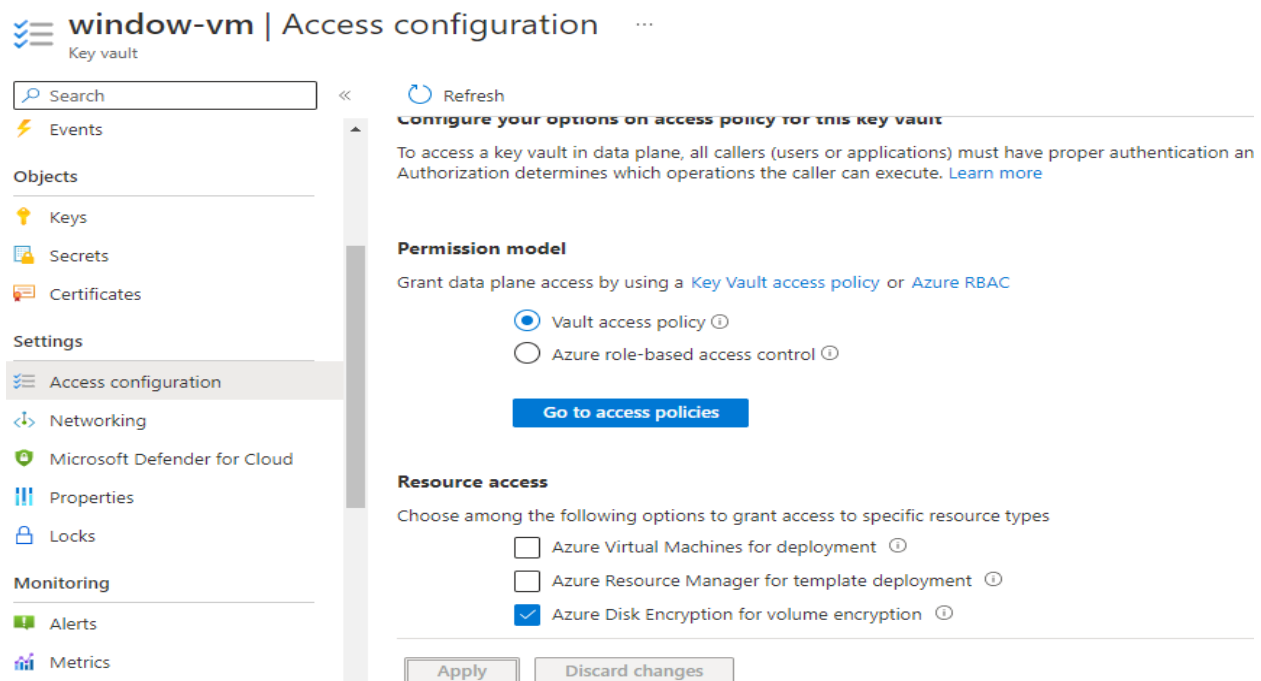
SSE with CMK

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 .

Encryption settings

Azure Disk Encryption (ADE) provides volume encryption for the OS and data disks. [Learn more about Azure Disk Encryption.](#)

Disks to encrypt ⓘ

None ▼

⚠ ADE settings can only be updated while the virtual machine is running. Start the virtual machine to update ADE settings. [Learn more](#)

We need to start vm to enable ade .

[Encryption.](#)

Disks to encrypt ⓘ

OS disk ▼

None

OS disk

OS and data disks

te, you need to
use an optional

[Create a key vault](#)

Key ⓘ

Select a key ▼

Version ⓘ

Select a key version ▼

We can select the disk to enable ade .