

AZURE LAB 5 (SSE)

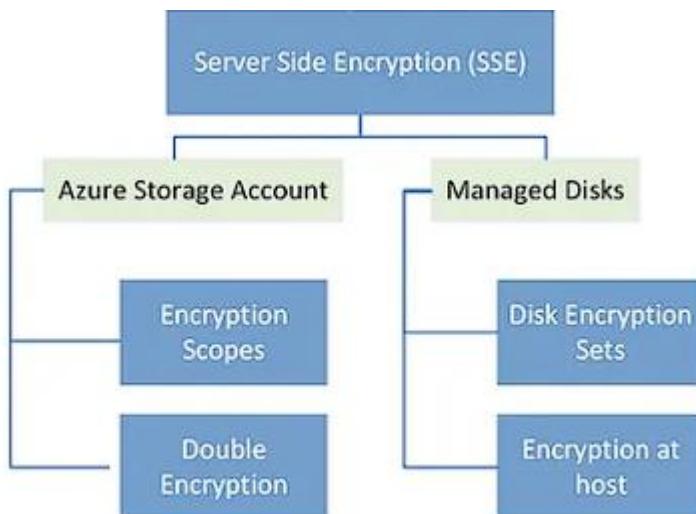
😊 SERVER-SIDE ENCRYPTION:

Server-side encryption (SSE) is a method used to encrypt data at rest on a server. It is a security measure employed to protect sensitive information stored on servers from unauthorized access or tampering. In the context of cloud computing and storage services, such as Amazon S3, Microsoft Azure Blob Storage, or Google Cloud Storage, server-side encryption is often implemented to enhance data security.

There are generally two types of server-side encryption:

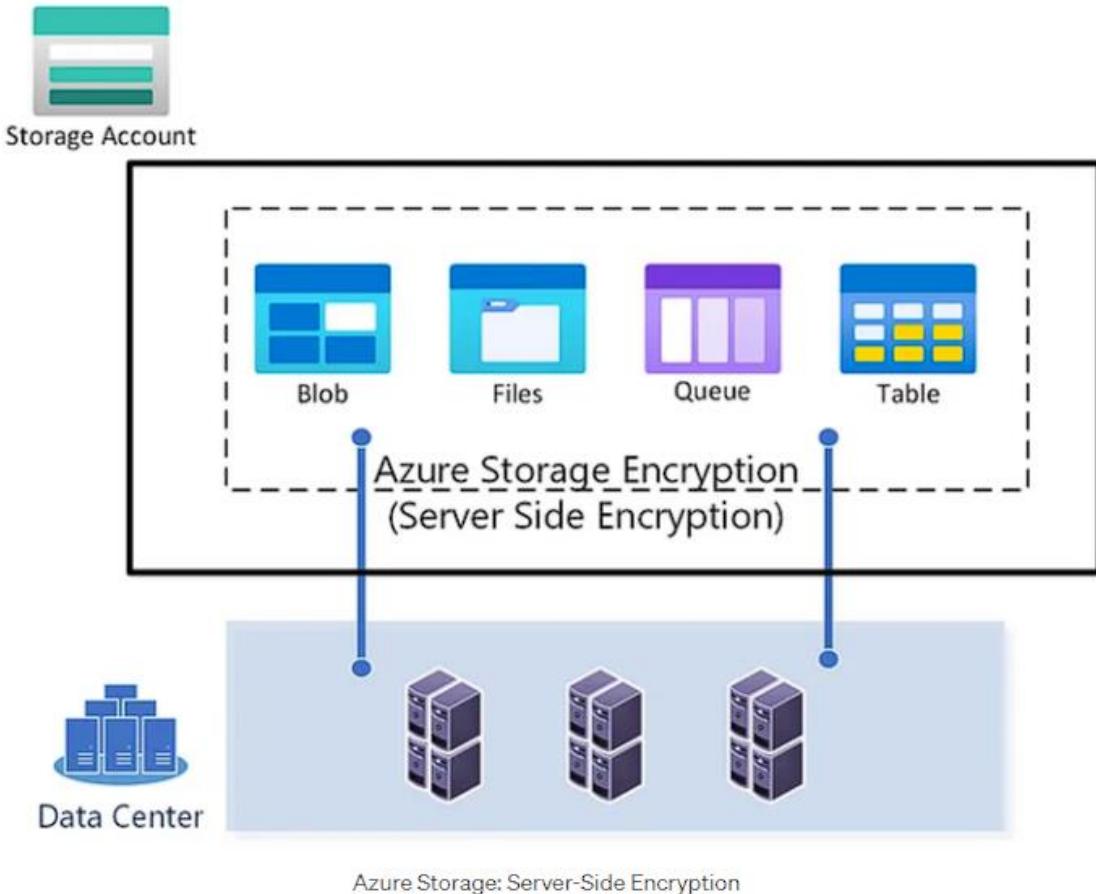
1. **Server-Side Encryption with Server-Managed Keys (SSE-S3, SSE-AES):** In this approach, the cloud service provider manages the encryption keys. The actual data is encrypted on the server before being stored, and the encryption keys are handled by the service provider. SSE-S3 is used in Amazon S3, and SSE-AES is a similar approach used in some other services.
2. **Server-Side Encryption with Customer-Provided Keys (SSE-C):** With this method, the customer provides and manages the encryption keys. The cloud service provider still encrypts the data on the server, but it uses the customer-supplied keys for encryption. This gives the customer greater control over the encryption keys.

In both cases, server-side encryption provides an additional layer of security for data stored on servers. Even if someone gains unauthorized access to the physical server or the underlying storage media, the encrypted data is meaningless without the corresponding encryption keys.



We know the actual data resides in Microsoft's data centre infrastructure and by default, data in Azure Storage accounts are encrypted at rest by using a feature called "**Azure Storage Encryption**" or "**Server-Side Encryption (SSE)**". It uses a symmetric AES256 key called **Data Encryption Key (DEK)** to encrypt your data at rest. This feature — **Server-Side Encryption (SSE)** generates a unique DEK for each blob, file, or queue message. It makes sense to encrypt large

amounts of data using a symmetric key(s) because it takes less computation time to encrypt or decrypt data using the same key.



Customer Managed Keys (CMK) and Platform Managed Keys (PMK):

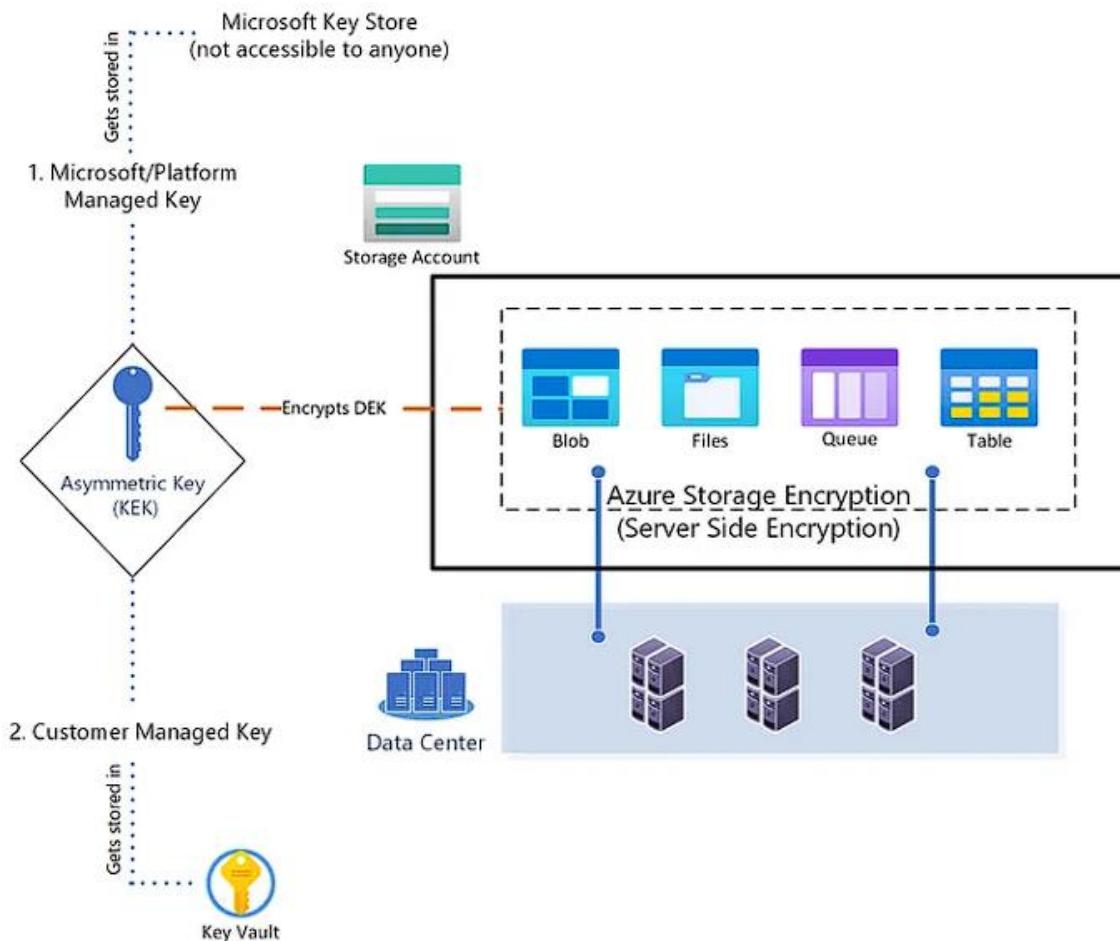
What if someone gets a handle on the Data Encryption Key (DEK)? We can take a step further in protecting DEK. Most cloud providers, including Azure, will protect DEK by encrypting with an asymmetric key called Key Encryption Key (KEK). It is kind of an encryption wrapper around DEK, usually called envelope or encryption wrapping. You can bring your own key (Customer Managed Key — CMK) [OR] rely on the Microsoft platform to generate a key (Platform Managed Key — PMK) to encrypt DEK. Customer Managed Keys (CMK) are typically stored in Azure Key Vault whereas PMK is stored in Microsoft Key Store which is not accessible to anyone.

Why do we have to protect DEK with an asymmetric key?

By using asymmetric encryption, encrypted DEKs can be unencrypted only by those with access to the CMK or PMK, mitigating the key exchange problem of symmetric algorithms.

If you are using CMK, the customer is responsible for managing keys including the creation, rotation, and revocation of keys, whereas, for PMK, Microsoft manages the keys for you and you don't need to worry about management tasks such as key rotation, backups or disaster recovery.

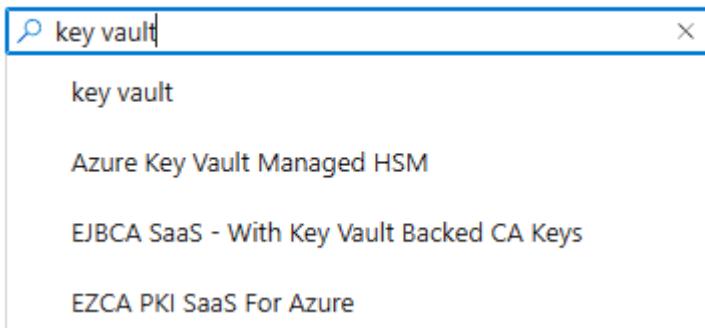
Typically, customers will use their own keys if they want to have an audit trail of when data is being encrypted and accessed and so on.



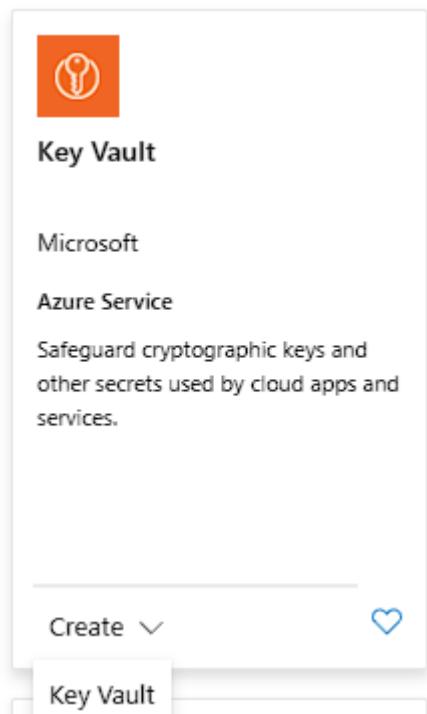
TO BEGIN WITH THE LAB

STEP 1: AZURE KEY VAULT

1. I've already prepared a virtual machine from my last lab which is **LAB 4**.
2. Now you need to go to the Azure Portal. There you need to navigate to **Azure Key Vault Service**.
3. This service will help you to store your keys.
4. Now on the portal click on create resource, then search key vault.



5. Select key vault service and click on create key vault.



6. Once you create a key vault page, select your resource group.
7. Then give a name to your key vault, and select your region.
8. Let the pricing tier be as Standard.
9. Then select days to retain deleted vaults to 7 days. Click next.
10. Then you need to enable purge protection.

Create a key vault

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *

Instance details

Key vault name * ⓘ

Region *

Pricing tier * ⓘ

Recovery options

Soft delete ⓘ

Days to retain deleted vaults * ⓘ

Purge protection ⓘ

<input checked="" type="radio"/> Disable purge protection (allow key vault and objects to be purged during retention period)
<input type="radio"/> Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

11. On the next page, in the permission model select Vault access policy.

Permission model

Grant data plane access by using a [Azure RBAC](#) or [Key Vault access policy](#)

- Azure role-based access control (recommended) ⓘ
- Vault access policy ⓘ

12. Keep all the aspects as they are and go to review and create.

13. Once the deployment is complete, go to resources.

Delete Cancel Redeploy Download Refresh

Your deployment is complete

Deployment name : appvault2711 Subscription : Free Trial Resource group : app-grp	Start time : 12/22/2023, 2:56:28 PM Correlation ID : 60a1f99c-60a2-4733-9a25-49cedc2c83a6
--	--

- > Deployment details
- < Next steps

[Go to resource](#)

14. Here you can see the details related to your key vault.

appvault2711

Key vault

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Access policies

Events

Objects

- Keys
- Secrets
- Certificates

Settings

- Access configuration
- Networking
- Microsoft Defender for Cloud
- Properties
- Locks

Upcoming TLS 1.0, 1.1 deprecation: Please enable support for TLS 1.2 on clients (applications/platform) to avoid any service impact. Learn more here.

Vault URI : https://appvault2711.vault.azure.net/
 Sku (Pricing tier) : Standard
 Directory ID : 30aa9099-b1e3-4652-abe8-06310e4b8029
 Directory Name : Default Directory
 Soft-delete : Enabled
 Purge protection : Disabled

Tags (edit) : Add tags

Get started Properties Monitoring Tools + SDKs Tutorials

Manage keys and secrets used by apps and services

Our recommendation is to use a vault per application per environment (Development, Pre-Production and Production). This helps you to not share secrets across environments and also reduces the threat in case of a breach.

Control access to key vault

Assign access policy and determine whether a given service principal, namely an application or user group, can perform different operations on key vault keys, secrets or certificates.

15. In the resources go to Access Control (IAM) and then there go to Role assignments. Now here you have to add a role for Key Vault Administrator.

demovaultkey0001 | Access control (IAM)

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription : 1

Privileged : 0

View assignments

All Job function (1) Privileged (0)

Search by name or email

Type : All Role : All Scope : All scopes Group by : Role

Name	Type	Role	Scope	Condition
Ritesh Behal behal.riteh@gmail.com#EXT#@behalesthsgr...	User	Key Vault Administrator	This resource	None

STEP 2: DISK ENCRYPTION SET

1. Now in the vault, from the objects click on the keys option

Objects

Keys

2. Initially you will have zero keys. So now you are going to create a key, for that click on Generate/import.

Name	Status	Expiration date
There are no keys available.		

3. Here you just need to give it a name and keep all the options as it is. Then hit on create.

Create a key

Options: Generate

Name: vmkey

Key type: RSA

RSA key size: 2048

Set activation date:

Set expiration date:

Enabled: Yes

Tags: 0 tags

Set key rotation policy: Not configured

Confidential Key Options:

- Exportable:
- Immutable:

Confidential operation policy:

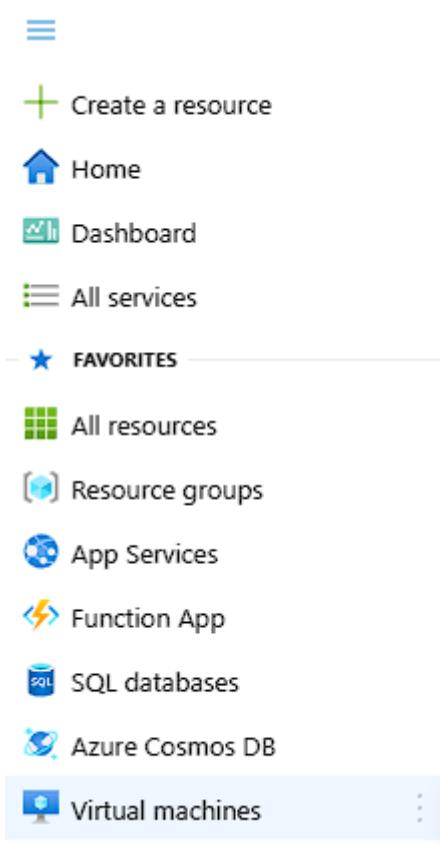
Create **Cancel**

4. Now you can see your key is successfully created.

Name	Status	Expiration date
vmkey	✓ Enabled	

The key 'vmkey' has been successfully created.

- Now you need to click on the hamburger icon on the top left of your screen and then navigate to virtual machines.



- Here you can see your virtual machine.

The screenshot shows the 'Virtual machines' blade with the following details:

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk count
WindowsVm	Virtual machine	Free Trial	WindowsVm_group	Central India	Running	Windows	Standard_D2s_v3	20.219.10.95	2

- Open your virtual machine and navigate to disks. In the disks, you can see that both your disks are encrypted with Server-Side Encryption with Platform Managed Keys.

The screenshot shows the 'Disks' blade with the following details:

LUN	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (MBps)	Encryption	Host caching
0	WindowsVm_OsDisk_1_b89a17a8ef0846e4b3cbd538ed44a	Premium SSD LRS	127	500	100	SSE with PMK	Read/write

LUN	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (MBps)	Encryption	Host caching
0	datadisk1	Premium SSD LRS	20	120	25	SSE with PMK	Read-only

- But now you are going to apply Server-Side Encryption with your key which you created earlier i.e. My customer-managed keys.
- Now you need to search disk encryption set. And choose this service.

Disk Encryption Sets

Disks

Disk Accesses

Disk Pools

Availability sets

Diagnostic settings

Diagnostic settings

Disks (classic)

10. Open it, currently, there will be no encryption sets, so you need to create one.

Disk Encryption Sets

Default Directory (pulkitkumar2711@gmail.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 0 to 0 of 0 records.

Name ↑↓ Resource group ↑↓

11. Click on Create, here select your resource group.
12. Then give a name to your encryption key.
13. Then keep the rest of the setting to default.
14. Now select your key vault.
15. Then select your key.
16. Then select a version, there will only be a single version attached to it. So, select that and move to review and create page.

Create a disk encryption set

your resources.

Subscription * ⓘ Free Trial

Resource group * ⓘ app-grp Create new

Instance details

Disk encryption set name * diskencryptionset

Region * ⓘ (Asia Pacific) Central India

Encryption type * ⓘ Encryption at-rest with a customer-managed key

Encryption key ⓘ

Select Azure key vault and key
 Select Azure key vault managed HSM and key (preview)
 Enter key from URI

Key Vault * ⓘ appvault2711

Manage selected vault
Create a key vault

Key * ⓘ vmkey

Create a key

Version * ⓘ Select a key version

User-assigned identity ⓘ Select an identity

Multi-tenant application ⓘ Select an application

! You are required to select the user-assigned managed identity first.

Auto key rotation ⓘ

Review + create

< Previous

Next : Tags >

17. Once the deployment of this complete then go to all resources.

✓ Your deployment is complete



Deployment name : Microsoft.DiskEncryptionSet-20231222151329
Subscription : Free Trial
Resource group : app-grp

Start time : 12/22/2023, 3:44:41 PM
Correlation ID : d81f99b3-45b9-42e6-a83b-b7dfe0ce61f3

> Deployment details

✓ Next steps

Go to resource

18. Now search for datadisk1, this is the disk that you created when the virtual machine was deployed.

A screenshot of the Azure Resource Explorer interface. At the top, there is a search bar with the word 'disk' and several filter options: 'Subscription equals all', 'Resource group equals all', 'Type equals all', 'Location equals all', and an 'Add filter' button. Below the filters, there are three buttons: 'Recommendations', 'Changed resources', and 'Unsecure resources'. On the right side, there is a dropdown menu for 'No grouping' and a refresh icon. The main table shows one resource: 'datadisk1' under the 'Disk' type, located in the 'WindowsVm_group' resource group, in 'Central India' location, and part of the 'Free Trial' subscription.

19. In the disk, under the settings option, navigate to Encryption.

A screenshot of the 'Encryption' settings page for a disk. The page has a navigation bar with 'Configuration', 'Size + performance', and 'Encryption' tabs. The 'Encryption' tab is highlighted with a grey background. Below the tabs, there is a message: 'Changes to encryption settings can only be made when the disk is unattached or the managing virtual machine(s) are deallocated.' At the bottom of the page, there are buttons for 'Save', 'Discard', 'Refresh', and 'Give feedback'.

20. Here you can see that there is an information related that says (Changes to encryption settings can only be made when the disk is unattached or the managing virtual machine(s) are deallocated)

21. So now go back to your virtual machine and stop it.

A screenshot of the 'Encryption' settings page for a virtual machine. The page includes a toolbar with 'Connect', 'Start', 'Restart', 'Stop', 'Hibernate (preview)', 'Capture', 'Delete', 'Refresh', 'Open in mobile', 'Feedback', and 'CLI / PS' buttons. Below the toolbar, there are buttons for 'Save', 'Discard', 'Refresh', and 'Give feedback'. A message box contains the text: 'Changes to encryption settings can only be made when the disk is unattached or the managing virtual machine(s) are deallocated.' At the bottom, there is a note about server-side encryption and a link to 'Learn more'.

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

Key management ⓘ

Platform-managed key

22. Once you have stopped and deallocated your virtual machine then go back to Encryption page. Here now you can see the message is gone and you can change the settings.

A screenshot of the 'Encryption' settings page for a disk. The page includes a toolbar with 'Save', 'Discard', 'Refresh', and 'Give feedback' buttons. Below the toolbar, there is a note about server-side encryption and a link to 'Learn more'. A message box contains the text: 'Changes to encryption settings can only be made when the disk is unattached or the managing virtual machine(s) are deallocated.' At the bottom, there is a note about server-side encryption and a link to 'Learn more'. The 'Key management' dropdown is set to 'Platform-managed key'.

23. So, change it from platform managed key to customer managed key. Then save it.

Key management ⓘ

Platform-managed key

Platform-managed key ⓘ

Platform-managed key

Customer-managed key ⓘ

diskencryptionset

Resource group: APP-GRP; Key vault: appvault2711; Key: vmkey

Platform-managed and customer-managed keys ⓘ

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

24. So, when you click on save, you'll see that it is showing you a failure.

! Failed to update disk

Failed to update disk 'datadisk1'. Error: Unable to access key vault resource
<https://appvault2711.vault.azure.net/keys/vmkey/0cb425ebd59d4cf1...>
to enable encryption at rest. Please grant get, wrap and unwrap key permissions to disk encryption set 'diskencryptionset'. Please visit <https://aka.ms/keyvaultaccessssecmk> for more information.

a few seconds ago

25. To avoid this failure, go to all resources, then navigate to disk encryption set.

All resources ⌂

Default Directory (pulkitkumar2711@gmail.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags Delete

disk encryption set Subscription equals all Resource group equals all Type equals all Location equals all Add filter

Name	Type	Resource group	Location	Subscription
diskencryptionset	Disk Encryption Set	app-grp	Central India	Free Trial

26. To can see this pop up, now what you have to do is simply click on it, and it will grant the required permission itself.

Delete Give feedback

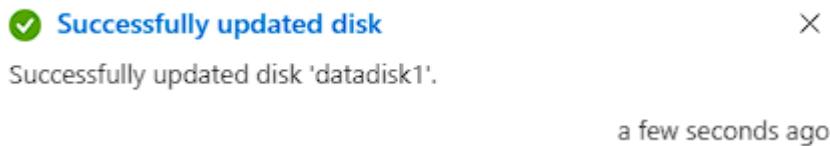
✖ To associate a disk, image, or snapshot with this disk encryption set, you must grant permissions to the key vault 'appvault2711'. →

27. As you can see from the notification, the required permission has been granted.

✓ Successfully granted permissions

Successfully granted permissions to the key vault 'appvault2711'.

28. Now if you go back to your disk and update your disk with customer manages keys, the action will perform smoothly. If you will see in the notification tab the disk has been updated successfully.



HENCE, THE LAB IS COMPLETED. 😊

For the deletion process go All Resources tab and delete your resources but do not delete Key Vault.

A screenshot of the Azure portal's "All resources" page. The page shows a list of 10 resources, all of which are marked as "Unsecure resources". The columns are Name, Type, Resource group, Location, and Subscription. The resources listed are:

Name	Type	Resource group	Location	Subscription
appvault2711	Key vault	app-grp	Central India	Free Trial
datadisk1	Disk	WindowsVm_group	Central India	Free Trial
diskencryptionset	Disk Encryption Set	app-grp	Central India	Free Trial
NetworkWatcher_centralindia	Network Watcher	NetworkWatcherRG	Central India	Free Trial
WindowsVm	Virtual machine	WindowsVm_group	Central India	Free Trial
WindowsVm-ip	Public IP address	WindowsVm_group	Central India	Free Trial
WindowsVm-msg	Network security group	WindowsVm_group	Central India	Free Trial
WindowsVm-vnet	Virtual network	WindowsVm_group	Central India	Free Trial
windowsvm929	Network interface	WindowsVm_group	Central India	Free Trial
WindowsVm_OsDisk_1_b89a17aef0846e4b3cbd538ed44a9c2	Disk	WINDOWSVM_GROUP	Central India	Free Trial