AZURE LAB 5 (SSE)

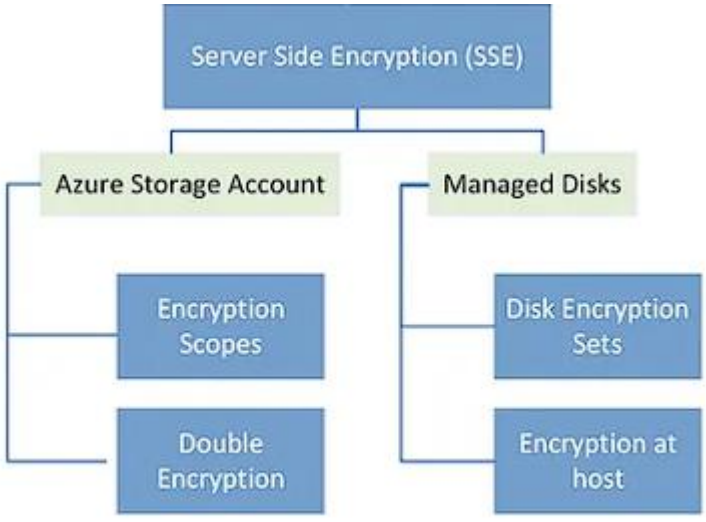
😁 SERVER-SIDE ENCRYPTION:

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:

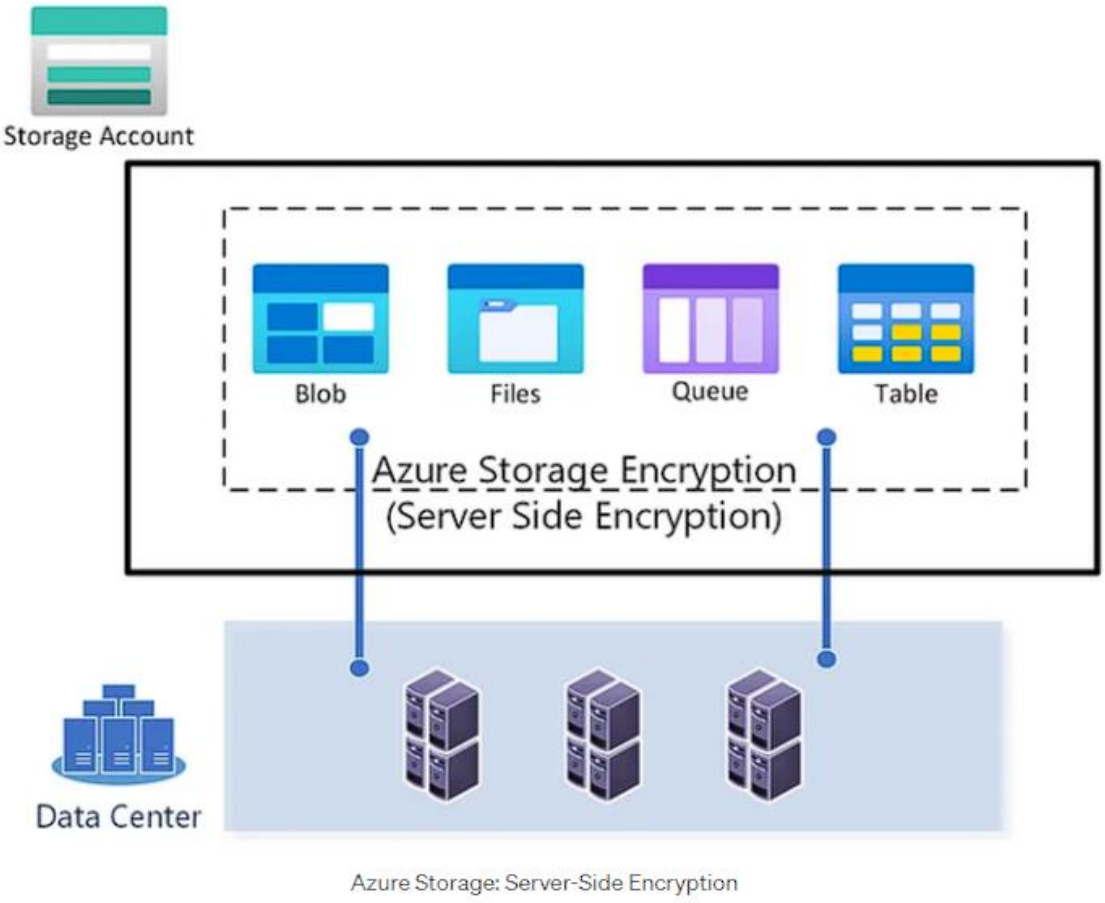
1. **Server-Side Encryption with Server-Managed Keys (SSE-S3, SSE-AES):** In this approach, the cloud service provider manages the encryption keys. The actual data is encrypted on the server before being stored, and the encryption keys are handled by the service provider. SSE-S3 is used in Amazon S3, 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.



Azure Storage: Server-Side Encryption

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

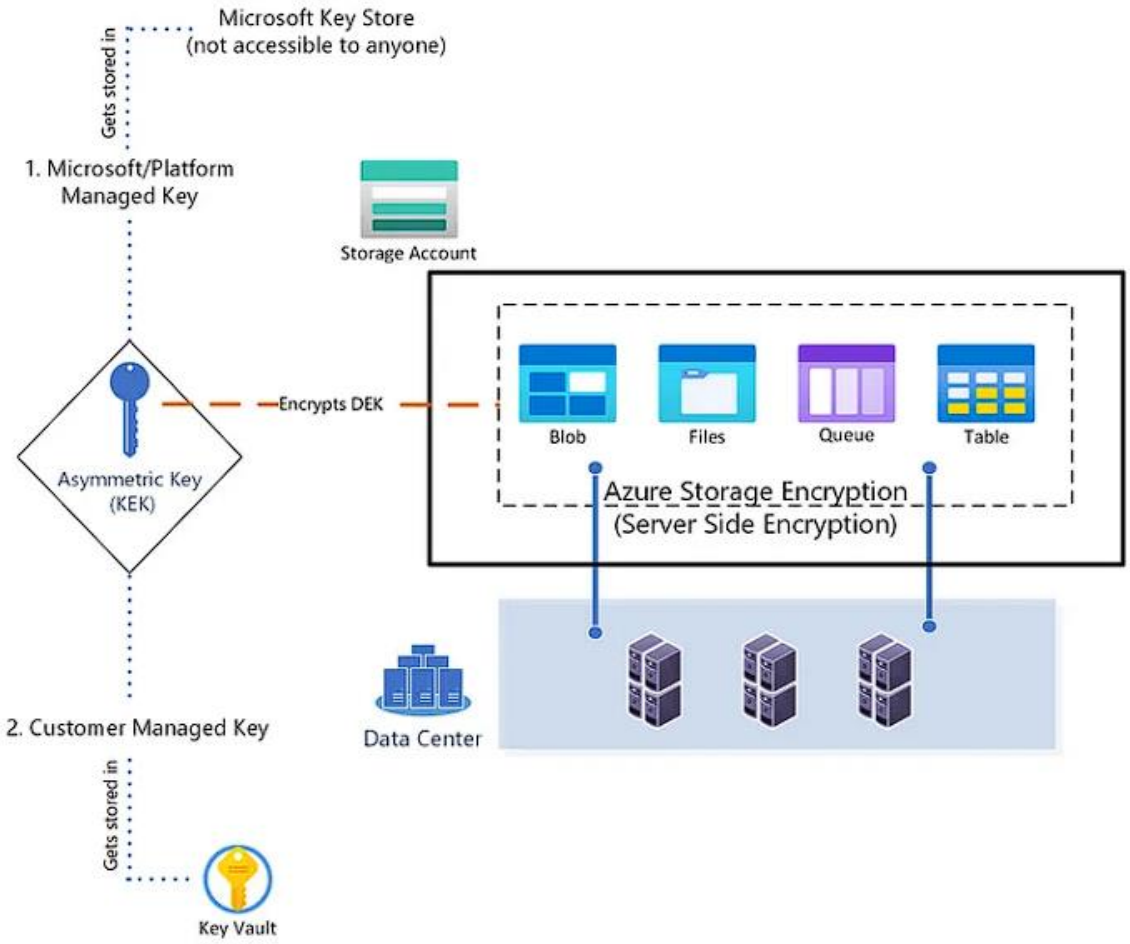
What if someone gets a handle on the Data Encryption Key (DEK)? We can take a step further in protecting DEK. Most cloud providers, including Azure, will protect DEK by encrypting with an asymmetric key called Key Encryption Key (KEK). It is kind of an encryption wrapper around DEK, usually called envelope 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.

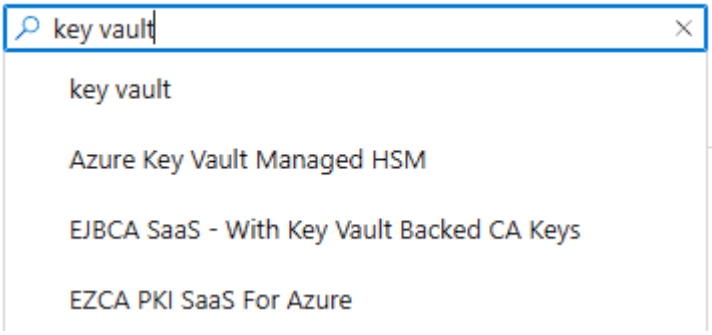


Azure Storage: Customer Managed Key and Microsoft (Platform) Managed Key

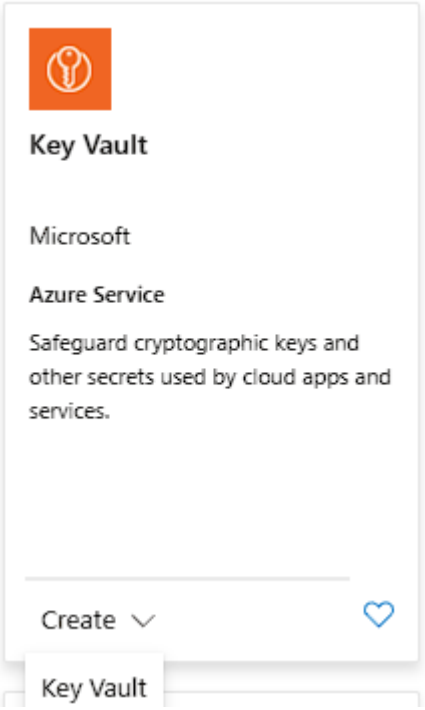
TO BEGIN WITH THE LAB

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 * : Free Trial

Resource group * : app-grp

Create new

Instance details

Key vault name * : appvault2711

Region * : Central India

Pricing tier * : Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete : Enabled

Days to retain deleted vaults * : 7

Purge protection :

- (●) Disable purge protection (allow key vault and objects to be purged during retention period)
- ( ) Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

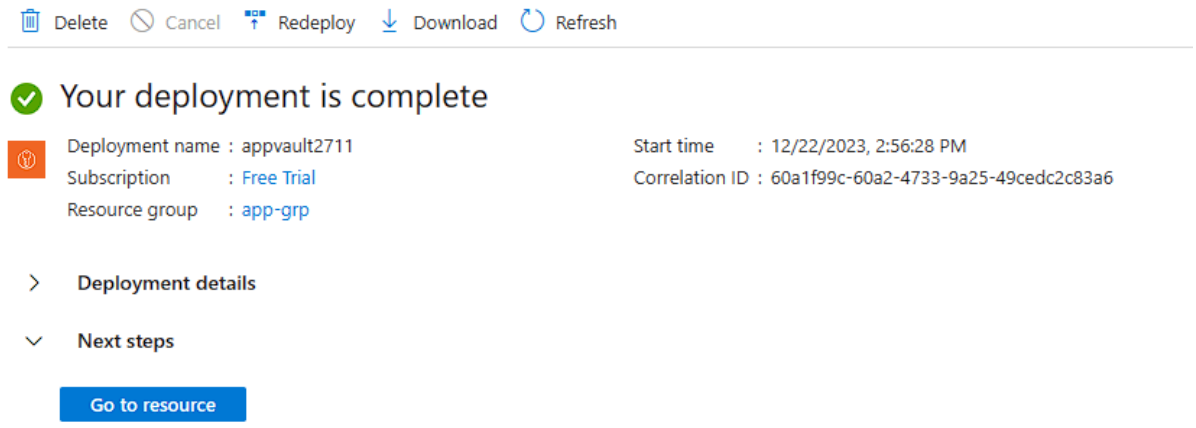
11. On the next page, in the permission model select Vault access policy.

Permission model

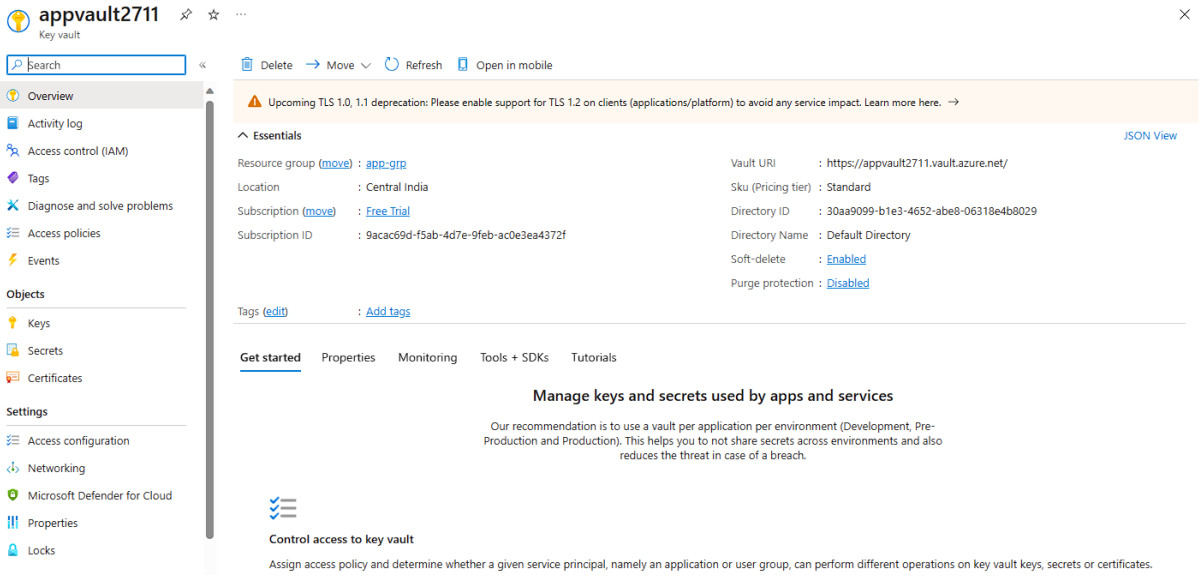
Grant data plane access by using a Azure RBAC or Key Vault access policy

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

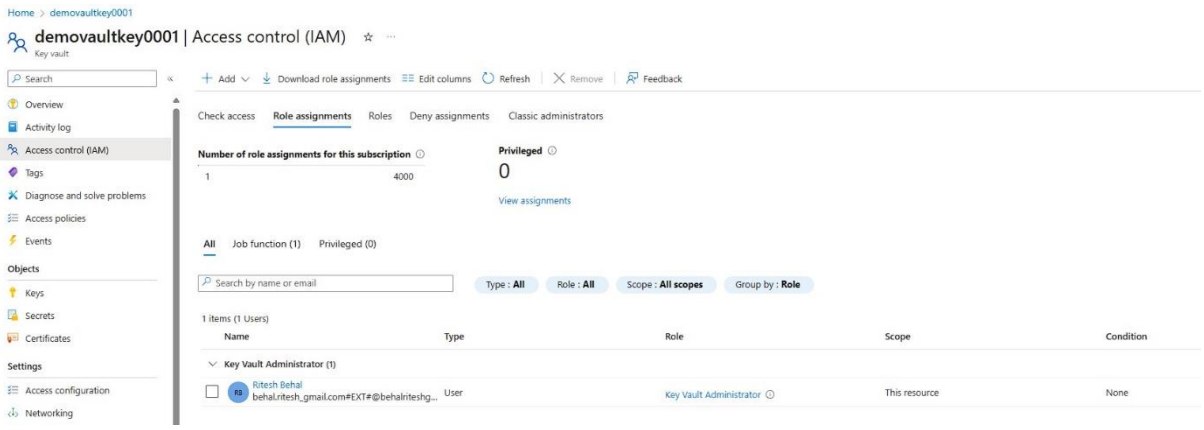
12. Keep all the aspects as they are and go to review and create.
13. Once the deployment is complete, go to resources.



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



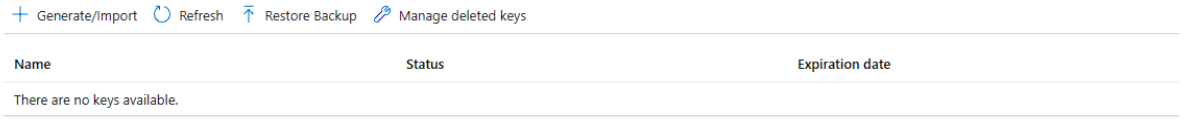
15. In the resources go to Access Control (IAM) and then there go to Role assignments. Now here you have to add a role for Key Vault Administrator.



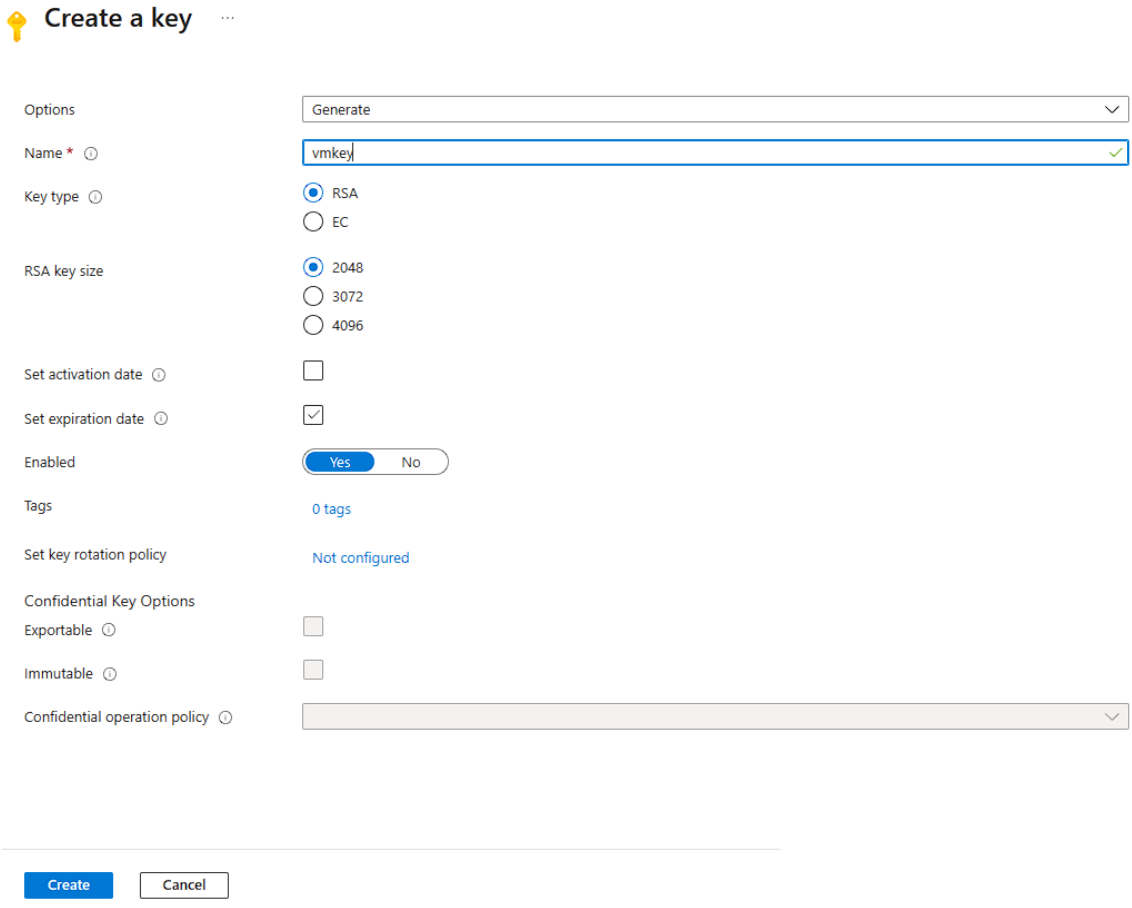
STEP 2: DISK ENCRYPTION SET

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

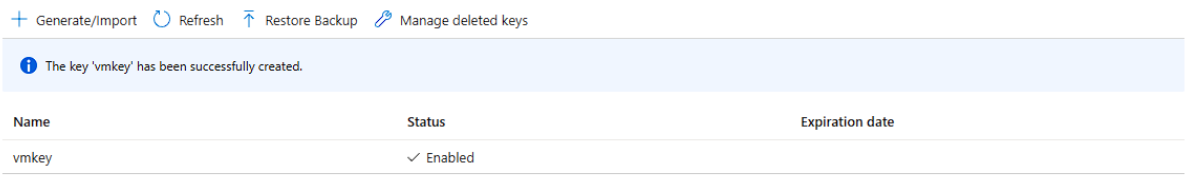
2. Initially you will have zero keys. So now you are going to create a key, for that click on Generate/import.



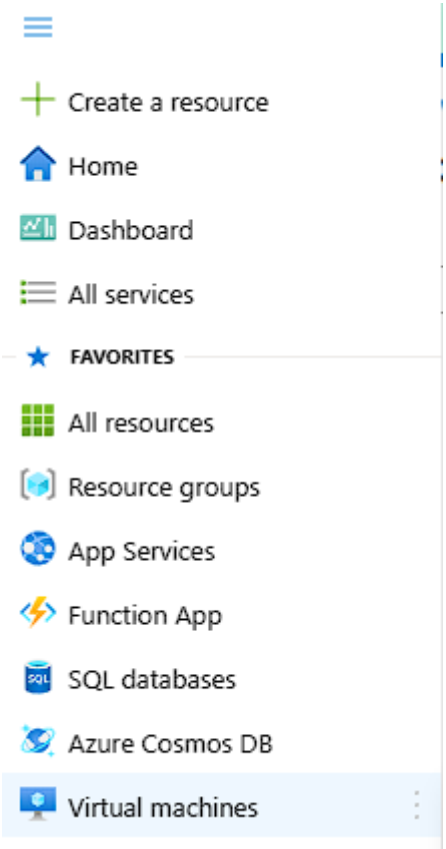
3. Here you just need to give it a name and keep all the options as it is. Then hit on create.



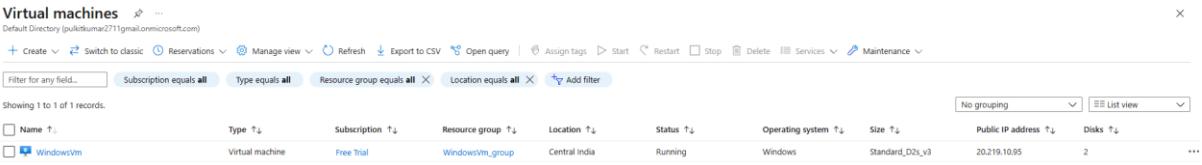
4. Now you can see your key is successfully created.



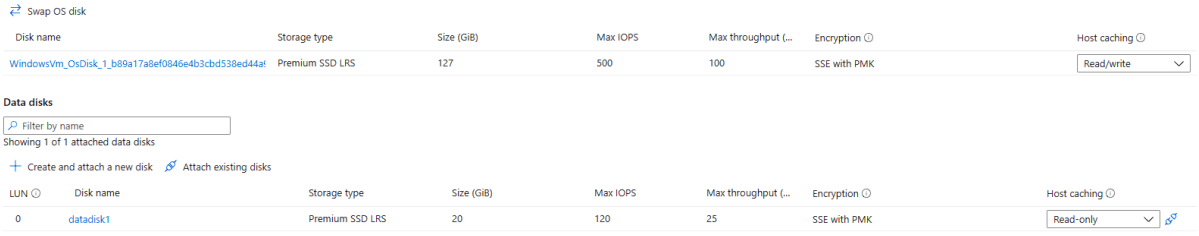
5. Now you need to click on the hamburger icon on the top left of your screen and then navigate to virtual machines.



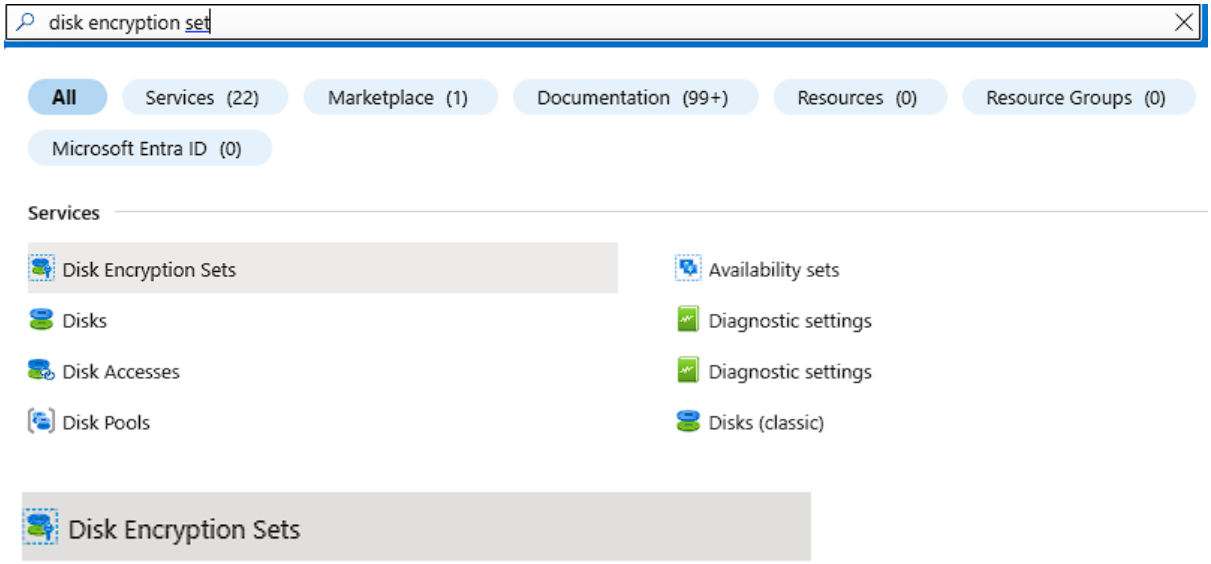
6. Here you can see your virtual machine.



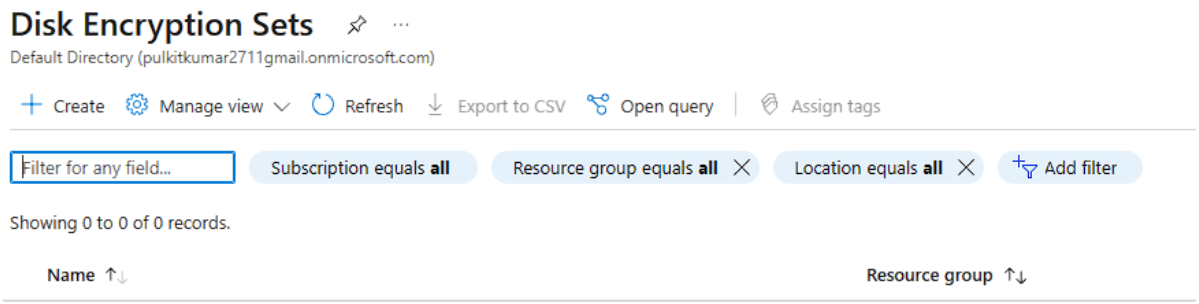
7. Open your virtual machine and navigate to disks. In the disks, you can see that both your disks are encrypted with Server-Side Encryption with Platform Managed Keys.



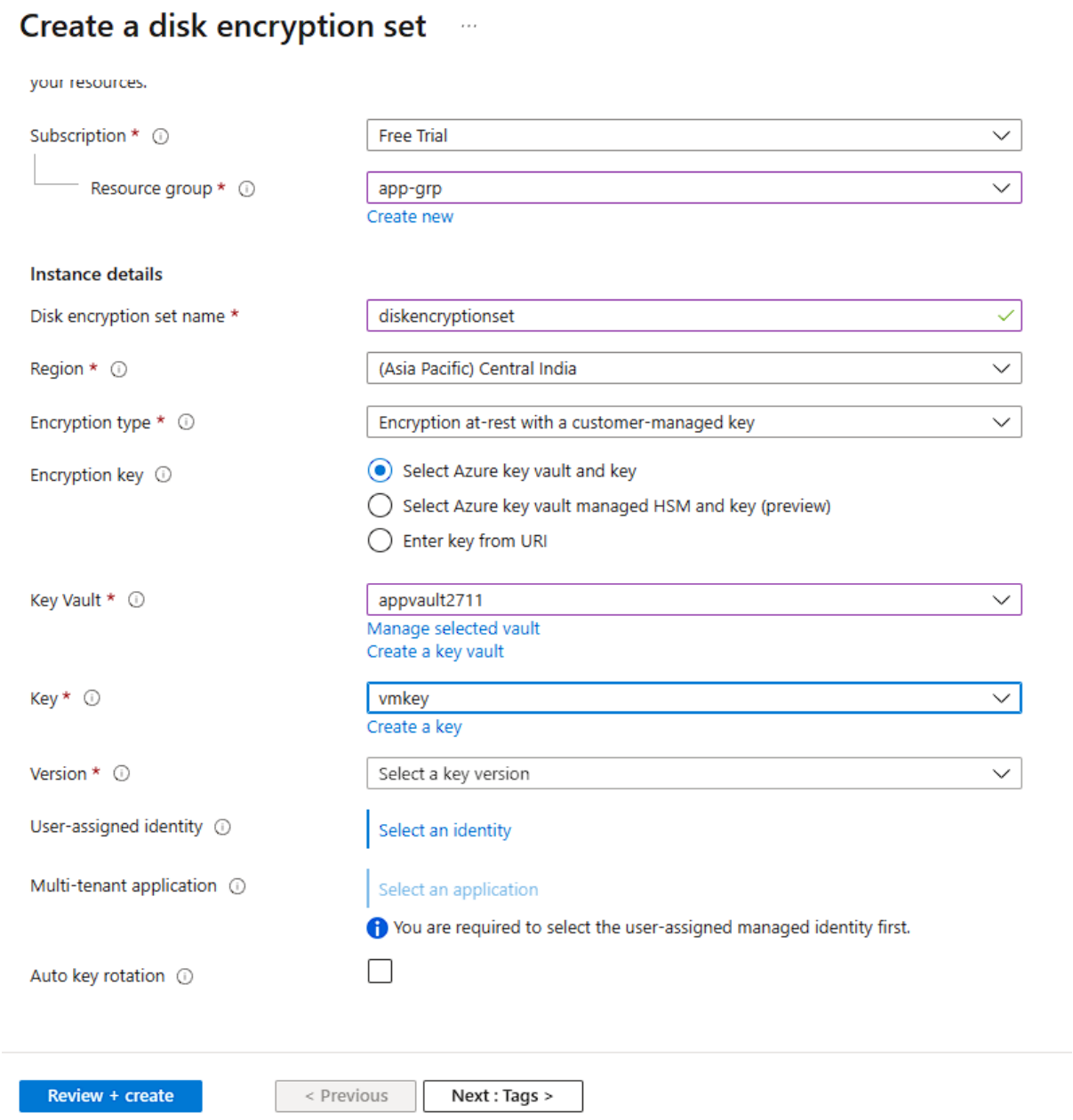
8. But now you are going to apply Server-Side Encryption with your key which you created earlier i.e. My customer-managed keys.
9. Now you need to search disk encryption set. And choose this service.



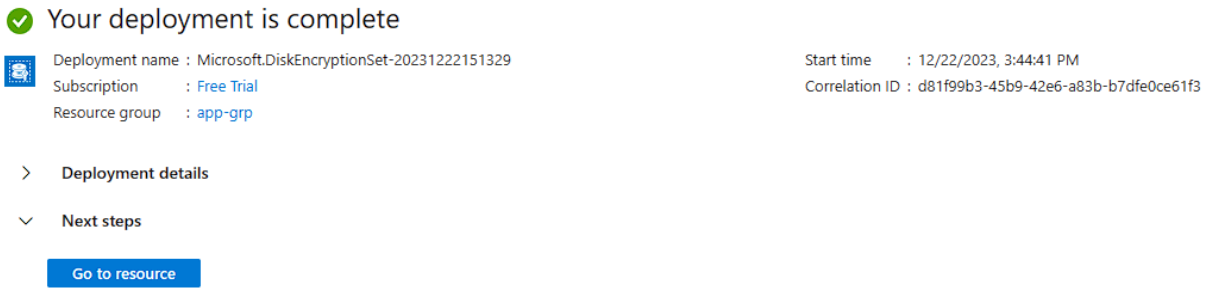
10. Open it, currently, there will be no encryption sets, so you need to create one.



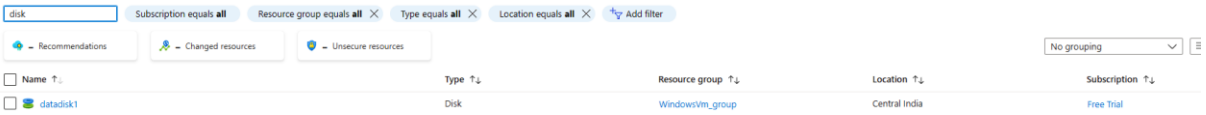
11. Click on Create, here select your resource group.
12. Then give a name to your encryption key.
13. Then keep the rest of the setting to default.
14. Now select your key vault.
15. Then select your key.
16. Then select a version, there will only be a single version attached to it. So, select that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



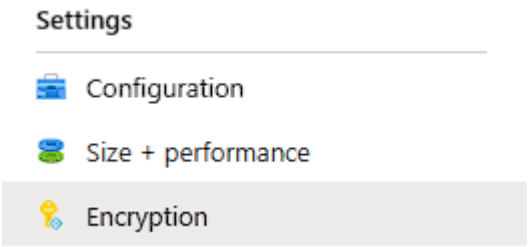
17. Once the deployment of this complete then go to all resources.



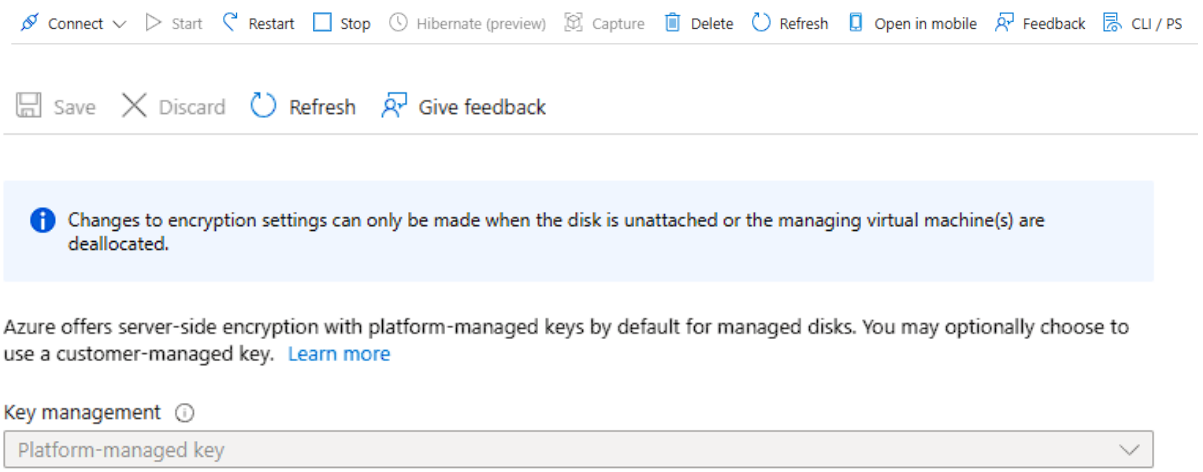
18. Now search for datadisk1, this is the disk that you created when the virtual machine was deployed.



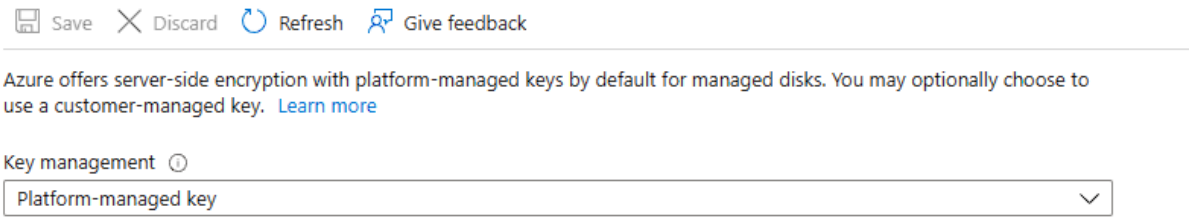
19. In the disk, under the settings option, navigate to Encryption.



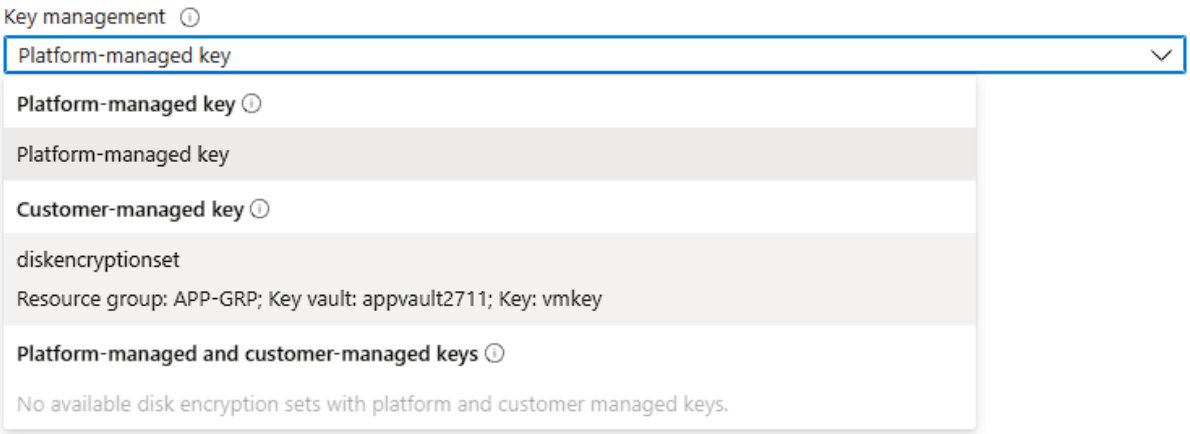
20. Here you can see that there is an information related that says (Changes to encryption settings can only be made when the disk is unattached or the managing virtual machine(s) are deallocated)
21. So now go back to your virtual machine and stop it.



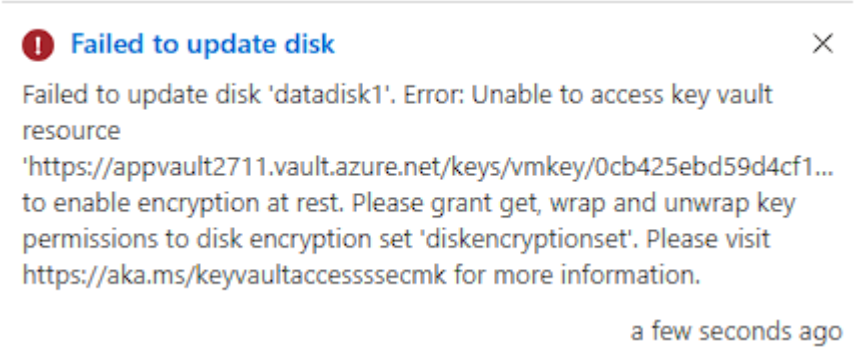
22. Once you have stopped and deallocated your virtual machine then go back to Encryption page. Here now you can see the message is gone and you can change the settings.



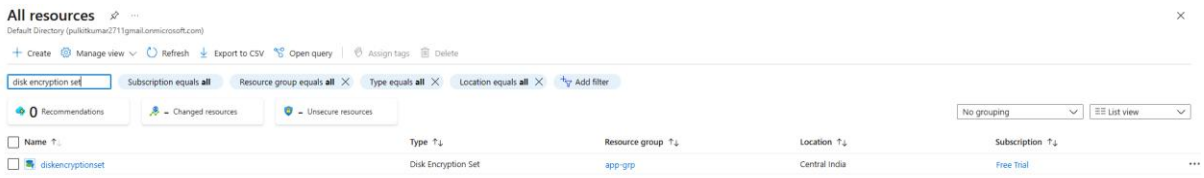
23. So, change it form platform managed key to customer managed key. Then save it.



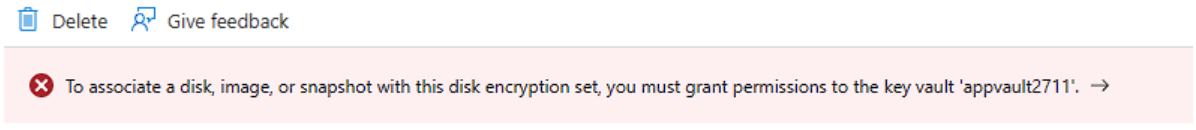
24. So, when you click on save, you'll see that it is showing you a failure.



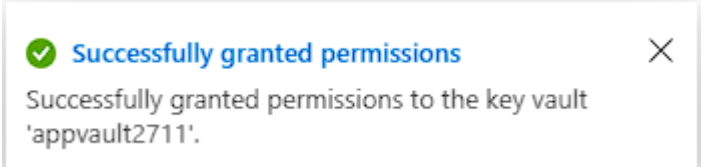
25. To avoid this failure, go to all resources, then navigate to disk encryption set.



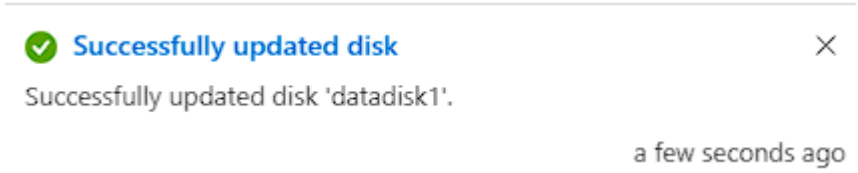
26. To can see this pop up, now what you have to do is simply click on it, and it will grant the required permission itself.



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



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.