Encryption Migration workaround for (SSE+CMK to ADE) & (ADE to SSE+CMK)_Encryption

Last updated by | Kevin Gregoire | Mar 29, 2022 at 11:47 AM PDT

Tags

cw.How-To	cw.Azure-Encryption

Contents

Summary

Microsoft released a feature called Server side encryption with customer managed keys (SSE + CMK) more info about it here: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption

Customer wants to migrate from SSE + CMK to ADE and vice versa, currently there is no migration process. This is a workaround will create a copy of the disk(s) without the encryption settings, which will allow the customer to migrate from ADE to SSE + CMK and vice versa.

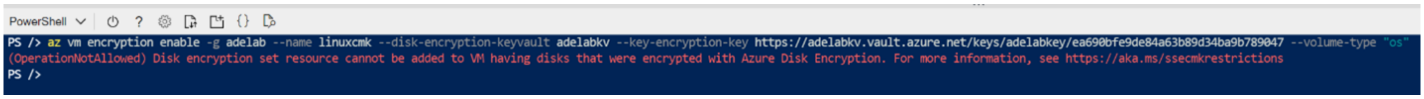
SSE + CMK is currently incompatible with Azure Disk Encryption (ADE).

Limitations

1. Disks that are part of an Encryption Set for SSE + CMK cannot be encrypted using ADE.
2. Disks Encrypted with ADE cannot be part of an Encryption Set for SSE + CMK.
3. Disks that are part of an Encryption Set cannot be removed from it.
4. All resources related to your customer-managed keys (Azure Key Vaults, disk encryption sets, VMs, disks, iamges, and snapshots) must be in the same subscription and region.
5. Disks, snapshots, and images encrypted with customer-managed keys cannot move to another resource group and subscription.

Scenario

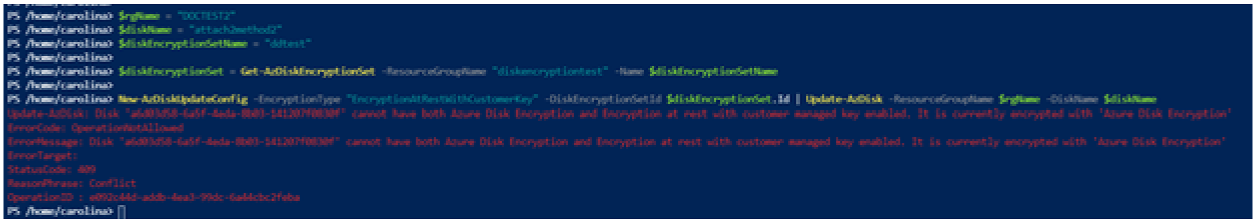
1. Customer already has SSE + CMK enabled they will get the following error when they are trying to encrypt with ADE.



```
PS /> az vm encryption enable -g adelab --name linuxcmk --disk-encryption-keyvault adelabkv --key-encryption-key https://adelabkv.vault.azure.net/keys/adelabkey/ea690bfe9de84a63b89d34ba9b789047 --volume-type "os"
(OperationNotAllowed) Disk encryption set resource cannot be added to VM having disks that were encrypted with Azure Disk Encryption. For more information, see https://aka.ms/ssecmkrestrictions
PS />
```

(OperationNotAllowed) Disk encryption set resource cannot be added to VM having disks that were encrypted with Azure Disk Encryption.

2. Customer already has ADE enabled they will get the following error when they are trying to encrypt with SSE + CMK.

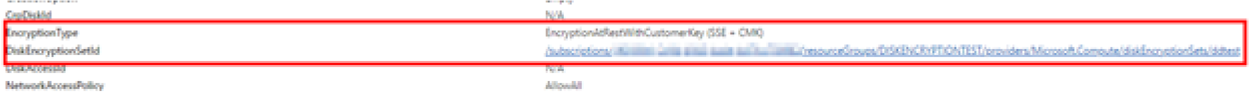


```
PS /home/carolina> $rgName = "DOCTEST2"
PS /home/carolina> $diskName = "attach2method2"
PS /home/carolina> $diskEncryptionSetName = "ddtest"
PS /home/carolina>
PS /home/carolina> $diskEncryptionSet = Get-AzDiskEncryptionSet -ResourceGroupName "diskencryptiontest" -Name $diskEncryptionSetName
PS /home/carolina>
PS /home/carolina> New-AzDiskUpdateConfig -EncryptionType "EncryptionAtRestWithCustomerKey" -DiskEncryptionSetId $diskEncryptionSet.Id | Update-AzDisk -ResourceGroupName $rgName -DiskName $diskName
Update-AzDisk: Disk "a6d03d58-6a5f-4eda-8b03-141207f0830f" cannot have both Azure Disk Encryption and Encryption at rest with customer managed key enabled. It is currently encrypted with 'Azure Disk Encryption'
ErrorCode: OperationNotAllowed
ErrorMessage: Disk "a6d03d58-6a5f-4eda-8b03-141207f0830f" cannot have both Azure Disk Encryption and Encryption at rest with customer managed key enabled. It is currently encrypted with 'Azure Disk Encryption'
ErrorTarget:
StatusCode: 409
ReasonPhrase: Conflict
OperationID : e092c44d-addb-4ea3-99dc-6a44cbc2feba
PS /home/carolina>
```

Disk cannot have both Azure Disk Encryption and Encryption at rest with customer managed key enabled. It is currently encrypted with 'Azure Disk Encryption'

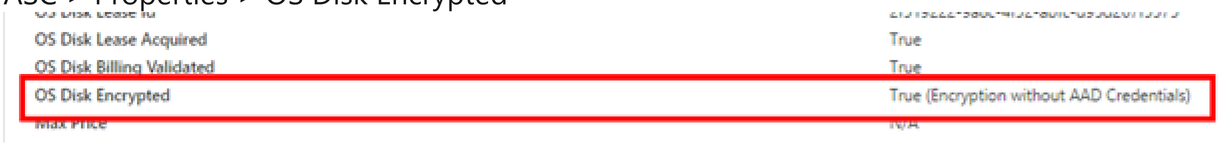
Verification

1. SSE + CMK
   ASC > Disks > Expand > Managed Disk > Click on the highlighted disk name > EncryptionType



CrpDiskId	N/A
EncryptionType	EncryptionAtRestWithCustomerKey (SSE + CMK)
DiskEncryptionSetId	/subscriptions/[redacted]/resourceGroups/DISKENCRYPTIONTEST/providers/Microsoft.Compute/diskEncryptionSets/ddtest
DiskAccessId	N/A
NetworkAccessPolicy	AllowAll

2. ADE
   ASC > Properties > OS Disk Encrypted



OS Disk Lease Acquired	True
OS Disk Billing Validated	True
OS Disk Encrypted	True (Encryption without AAD Credentials)
Max Price	N/A

Workaround

Copy the disk and attach it to the VM.

1. Follow (https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-upload-vhd-to-managed-disk-powershell#copy-a-managed-disk ↗)
2. Remove any configuration pointing to mount the SSE+CMK disk.
3. Detach the SSE+CMK disk from the VM.
4. Attach the newly created disk to the VM.
5. Configure the New disk to be mounted on boot.
6. Install ADE normally on the VM.

Need additional help or have feedback?

To engage the Azure Encryption SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the **Azure Encryption SMEs** for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **Azure Encryption Feedback** form to submit detailed feedback on improvements or new content ideas for Azure Encryption. ***Please note*** the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.	Use the **Azure Encryption Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!