User Encryption Settings in the VM Model are not Supported_Encryption

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

Tags	
cw.Azure-Encryption	cw.How-To

Contents

- Symptom
- Root Cause Analysis
- Mitigation

- Need additional help or have feedback?

Symptom

When you have a VM that is encrypted with Single Pass, but it was previously encrypted with Dual Pass and you try to attach a data disk, you will be seeing this error message: **Failed to update virtual machine 'DPVM'. Error: User encryption settings in the VM model are not supported. Please upgrade Azure Disk Encryption extension version and clear encryption settings in the VM model.**

Root Cause Analysis

When encrypting with Dual Pass, the encryption settings are stored in the VM model. If you disable the Dual Pass Encryption, and then rerun the command for encrypting with Single Pass, the operation will be allowed, but the VM will still have the encryption settings from the previous encryption. Once you apply a change to the VM, i.e by attaching a data disk, this will be identified, and you will see the error message **Failed to update virtual machine 'VM'. Error: User encryption settings in the VM model are not supported. Please upgrade Azure Disk Encryption extension version and clear encryption settings in the VM model.** Please keep in mind that migration from Dual Pass to Single Pass is not a supported scenario, even if the operation is allowed.

Mitigation

A clear encryption settings will take care of removing the settings in the VM Model that remained in the VM from the Dual Pass encryption.

Removing the old DP encryption settings artifact should only be done only in the following circumstances:

- DP has been fully disabled and removed
- The encryption settings block is already null with Enabled=False
- Single pass encryption has completed successfully on the VM

If that criteria is met, the old dual pass encryption settings artifact can be removed using the following steps:

```
$vm = Get-AzVM -ResourceGroupName $VMRGname -VMName $vmName
$vm.StorageProfile.OsDisk.EncryptionSettings=$null
$vm | Update-AzVM
```

Before (EncryptionSettings is a DiskEncryptionSettings object):

```
$vm.StorageProfile.OsDisk.EncryptionSettings |format-custom

class DiskEncryptionSettings
{
  DiskEncryptionKey =
  KeyEncryptionKey =
  Enabled = False
}
```

After (EncryptionSettings is null, with no DiskEncryptionSettings object):

```
$vm.StorageProfile.OsDisk.EncryptionSettings
$vm.StorageProfile.OsDisk

OsType                 : Windows
EncryptionSettings     :
Name                   : myvm_OsDisk_1_955aa7be282a4b7684a23bc22dafa94b
Vhd                    :
Image                  :
Caching                : ReadWrite
WriteAcceleratorEnabled :
DiffDiskSettings       :
CreateOption           : FromImage
DiskSizeGB             : 127
ManagedDisk            : Microsoft.Azure.Management.Compute.Models.ManagedDiskParameters
```

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!