Disable Dual Pass and Enable Single Pass ADE Extension_Encryption

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

Tags

cw.Azure-Encryption cw.How-To

Contents

Summary

In this TSG you will learn how to disable ADE Dual Pass and Enable Single Pass in Windows. Steps can be found here How to Disable ADE DP and Enable ADE SP

Note: If you are seeking to migrate from Dual Pass to Single Pass we highly recommend using the Migration steps as per how to - Migrate From Dual Pass to Single Pass extension or public document Upgrading the Azure Disk Encryption version

Note: These instructions are currently for Windows only. On Linux, decrypting volumes is not supported once the OS drive has been encrypted.

Warning: If the VM was DP encrypted using the AAD Client Certificate option (rather than client secret/password) these steps do not include the instructions needed to remove the old client certificate information from the VM model.

Instructions

On Windows, a VM that has been encrypted with AAD credentials ("dual pass" or "DP") can be fully decrypted and returned to a clean start state, and then it can be re-encrypted without AAD credentials ("single pass" or "SP") using the following sequence:

1. Enable DP (with AAD credentials)

```
$VMRGName = "myrg"
$vmName = "myvm"
$aadClientID = "myaadclient"
$aadClientSecret = "myaadsecret"
$KeyVaultName = "mykv"
$keyEncryptionKeyName = "mykek"
$diskEncryptionKeyVaultUrl = "https://mykv.vault.azure.net/"
$KeyVaultResourceId = "/subscriptions/abc/resourceGroups/myrg/providers/Microsoft.KeyVault/vaults/mykv"

Set-AzVmDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $vmName -AadClientID $aadClientID -A
```

Expected result:

```
        Enable AzureDiskEncryption on the VM
        This cmdlet prepares the VM and enables encryption which may reboot the machine and takes 10-15 m
        Please save your work on the VM before confirming. Do you want to continue?
        [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
        RequestId IsSuccessStatusCode StatusCode ReasonPhrase
        --------- ------------------- ---------- ------------
        True         OK OK
        $vm = Get-AzVM -ResourceGroupName $VMRGName -VMName $vmName
        $vm.StorageProfile.OsDisk.EncryptionSettings |format-custom

        class DiskEncryptionSettings
        {
        DiskEncryptionKey =
        class KeyVaultSecretReference
        {
        SecretUrl =
    https://myvault.vault.azure.net/secrets/placeholdersecret
        SourceVault =
        class SubResource
    {
    Id = /subscriptions/abc/resourceGroups/myrg/providers/Microsoft.KeyVault/vaults/mykv
        }
        }
        KeyEncryptionKey = mykek
        Enabled = True
        }
```

2. Disable DP Encryption

```
Disable-AzVMDiskEncryption -ResourceGroupName $VMRGName -VMName $vmName -Force
```

Expected result (encryption settings null, but extension still associated with VM model):

```
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
--------- ------------------- ---------- ------------
                       True         OK OK


PS > $vm = Get-AzVM -ResourceGroupName $VMRGname -VMName $vmName
PS > $vm.StorageProfile.OsDisk.EncryptionSettings |format-custom

   class DiskEncryptionSettings
{
DiskEncryptionKey =
KeyEncryptionKey =
Enabled = False
}

   PS > $vm.Extensions[0]

   ForceUpdateTag              :
   Publisher                   : Microsoft.Azure.Security
   VirtualMachineExtensionType : AzureDiskEncryption
   TypeHandlerVersion          : 1.1
   AutoUpgradeMinorVersion     : True
   Settings                    : {VolumeType, EncryptionOperation, SequenceVersion}
   ProtectedSettings           :
   ProvisioningState           : Succeeded
   InstanceView                :
   Id                          : /subscriptions/abc/resourceGroups/myrg/providers/M
                               icrosoft.Compute/virtualMachines/myvm/extensions/AzureDiskEncryption
   Name                        : AzureDiskEncryption
   Type                        : Microsoft.Compute/virtualMachines/extensions
   Location                    : eastus2euap
   Tags                        :
```

3. Remove DP Extension

```
Remove-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -Force
```

Expected result (encryption settings still null, extension is now also removed from the VM model):

```
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
--------- ------------------- ---------- ------------
                       True         OK OK

PS > $vm = Get-AzVM -ResourceGroupName $VMRGname -VMName $vmName
PS > $vm.StorageProfile.OsDisk.EncryptionSettings |format-custom

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

4. Enable SP (without AAD credentials)

Enabling "single pass" is done by **not** including AAD parameters in the call to Set-AzVMDiskEncryptionExtension

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $vmName -DiskEncryptionKeyVaultUrl $d
```

Expected Result:

Note: The cleared dual pass encryption settings block is still present in the VM model even after single pass encryption completes. This leftover fragment of dual pass encryption will be removed in the next step

```
Enable AzureDiskEncryption on the VM
This cmdlet prepares the VM and enables encryption which may reboot the machine and takes 10-15 minutes to
Please save your work on the VM before confirming. Do you want to continue?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

RequestId IsSuccessStatusCode StatusCode ReasonPhrase
--------- ------------------- ---------- ------------
                       True         OK OK


PS > $vm = Get-AzVM -ResourceGroupName $VMRGname -VMName $vmName
PS > $vm.StorageProfile.OsDisk.EncryptionSettings |format-custom

class DiskEncryptionSettings
{
DiskEncryptionKey =
KeyEncryptionKey =
Enabled = False
}

PS > $vm.Extensions[0]


ForceUpdateTag              :
Publisher                   : Microsoft.Azure.Security
VirtualMachineExtensionType : AzureDiskEncryption
TypeHandlerVersion          : 2.2
AutoUpgradeMinorVersion     : True
Settings                    : {SequenceVersion, KeyEncryptionKeyURL, KeyVaultResourceId, AADClientID...}
ProtectedSettings           :
ProvisioningState           : Succeeded
InstanceView                :
Id                          : /subscriptions/abc/resourceGroups/myrg/providers/M
                            icrosoft.Compute/virtualMachines/myvm/extensions/AzureDiskEncryption
Name                        : AzureDiskEncryption
Type                        : Microsoft.Compute/virtualMachines/extensions
Location                    : eastus2euap
Tags                        :
```

5. Remove DP Encryption Settings

Immediately after the VM has been properly single pass encrypted, it will still have a leftover encryption settings block with Enabled=False. Removing this leftover artifact will complete the migration from dual to single pass.

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!