Data Disks get Skipped During Encryption_Encryption

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

Tags

cw.Azure-Encryption cw.TSG

Contents

Symptom

When encrypting data disks sometimes they get silently skipped during encryption. Specifically storage space disks and data disks for Windows Server 2012 are at a higher risk of getting skipped. VMs that were already encrypted will not find their disks getting decrypted but new deployments or scale outs of existing VMSS might run into volumes being skipped for encryption. By checking the logs, you will see a message like the following

```
BitlockerOperations::IntializeMachineVolumes Skipping Volume Backed by VHD: VolumeName: H:\, VolumeLabel: Data
BitlockerOperations::IntializeMachineVolumes Skipping Volume Backed by VHD: VolumeName: G:\, VolumeLabel: Data
```

```
2021-03-11T07:24:20.2729355Z    [Info]: Disk Location  found for volume
2021-03-11T07:24:20.2885663Z    [Info]: IsVolumeBackedByVHD: \\?\Volume{4b0c548a-151c-4cb0-b6a0-86b12375f779}\ is backed by a
VHD. Location: NULL
2021-03-11T07:24:20.2885663Z    [Info]: EncryptableVolume initialized: VolumeName: H:\, VolumeLabel: DataB1, VolumeLetter: H:,
VolumeId: \\?\Volume{4b0c548a-151c-4cb0-b6a0-86b12375f779}\, BootVolume: False, UseWin32Volume False
2021-03-11T07:24:20.2885663Z    [Info]: BitlockerOperations::IntializeMachineVolumes Skipping Volume Backed by VHD: VolumeName:
H:\, VolumeLabel: DataB1, VolumeLetter: H:, VolumeId: \\?\Volume{4b0c548a-151c-4cb0-b6a0-86b12375f779}\, BootVolume: False,
UseWin32Volume False
2021-03-11T07:24:20.3198152Z    [Info]: GetDeviceNumbersForVolume for:\\?\Volume{d16bc167-bcb1-4a6d-a2a2-d668ef843672}
```

Cause

A regression has been found in the 2.2.0.37 version of the extension and this leads to data disks sometimes get silently skipped during encryption process.

Mitigation

To help mitigate this issue we have deployed the bug-free previous version (2.2.0.36) to 2.1.0.36 (note that it's 2.1, not 2.2). Customers that run into this issue can mitigate it by:

- Removing the 2.2.0.37 version via the Remove-azVMExtension cmdlet (or its vmss equivalent)
- Adding back the extension with version 2.1 and autoupgrade disabled. (Examples below)

```
Set-AzVmssDiskEncryptionExtension .... -TypeHandlerVersion 2.1 -DisableAutoUpgradeMinorVersion
Set-AzVmDiskEncryptionExtension .... -TypeHandlerVersion 2.1 -DisableAutoUpgradeMinorVersion
```

Steps

1. Run Remove-AzVMDiskEncryptionExtension -ResourceGroupName "MyResourceGroup" -VMName "MyTestVM"

2. Run Encryption script specifying the version 2.1.0.x

```
$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MySecureVM';
$KeyVaultName = 'MySecureVault';
$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
$KeyVaultResourceId = $KeyVault.ResourceId;
$sequenceVersion = [Guid]::NewGuid();
Set-AzVMDiskEncryptionExtension -TypeHandlerVersion 2.1 -DisableAutoUpgradeMinorVersion -ResourceGroupNa
```

For more information, please refer to IcM Storage pool virtual disk was mistakenly considered backedbyvhd and encryption skipped

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!