Get Keyvault Secret Used by Encrypted VM_Encryption

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

Tags

cw.Azure-Encryption cw.How-To

Contents

Scenario

When a customer wants to recover an encrypted VHD and should know the secret to download the BEK file and unlock/recover the VHD.

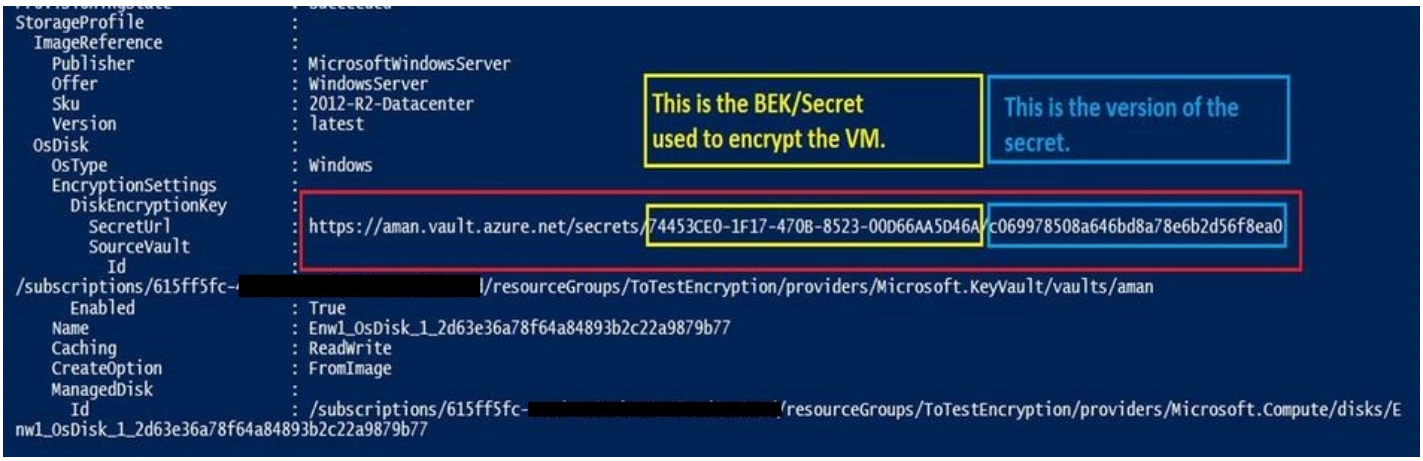
Windows VM

1. The encryption settings are exposed in VM Model. Use the following PowerShell commands to get the VM model details which contains the encryption settings for the VM under the StorageProfile.

```
$rgName = "<RESOURCE GROUP>"
$kvrgName = 'ToTestEncryption'
$vmName = "<VM NAME>"
$KeyVaultName = "<KEY VAULT NAME>"
$keyvaultkeyname = "<KEY NAME>"
$location = "<LOCATION>"

Get-AzVM -ResourceGroupName $rgName -Name $vmName -DisplayHint Expand
```

2. The SecretUrl contains the BEK file name and the version of the secret.



3. The second pull that we can do to narrow down the search if the "Expand" feature does not work from above.

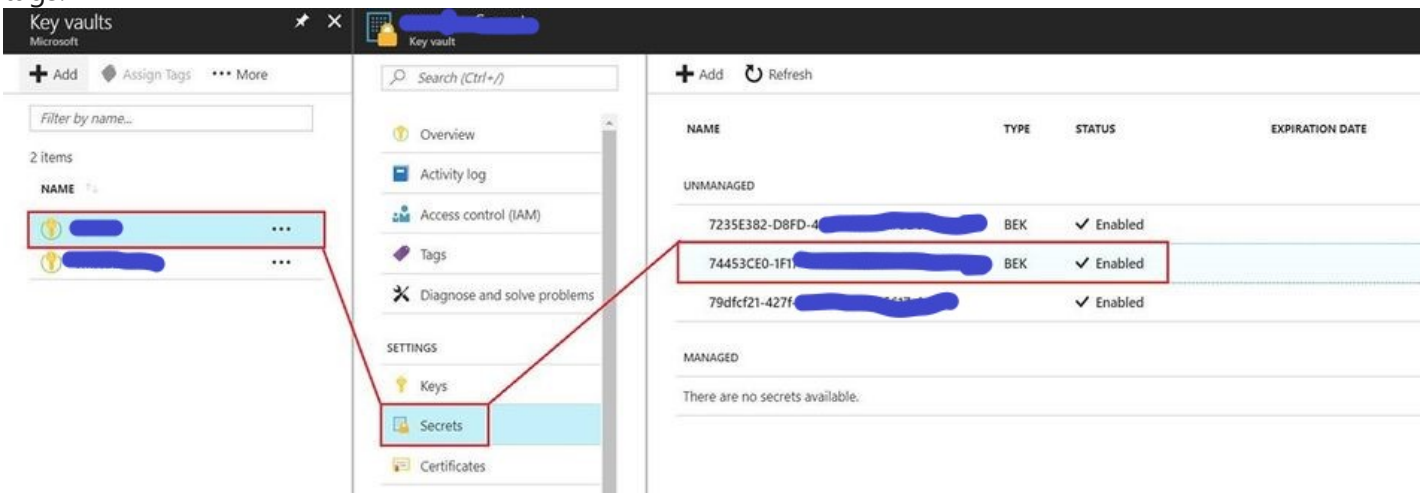
```
$vm = Get-AzVM -ResourceGroupName $rgName -Name $vmName
$vm.StorageProfile.OsDisk.EncryptionSettings.DiskEncryptionKey.SecretUrl
```

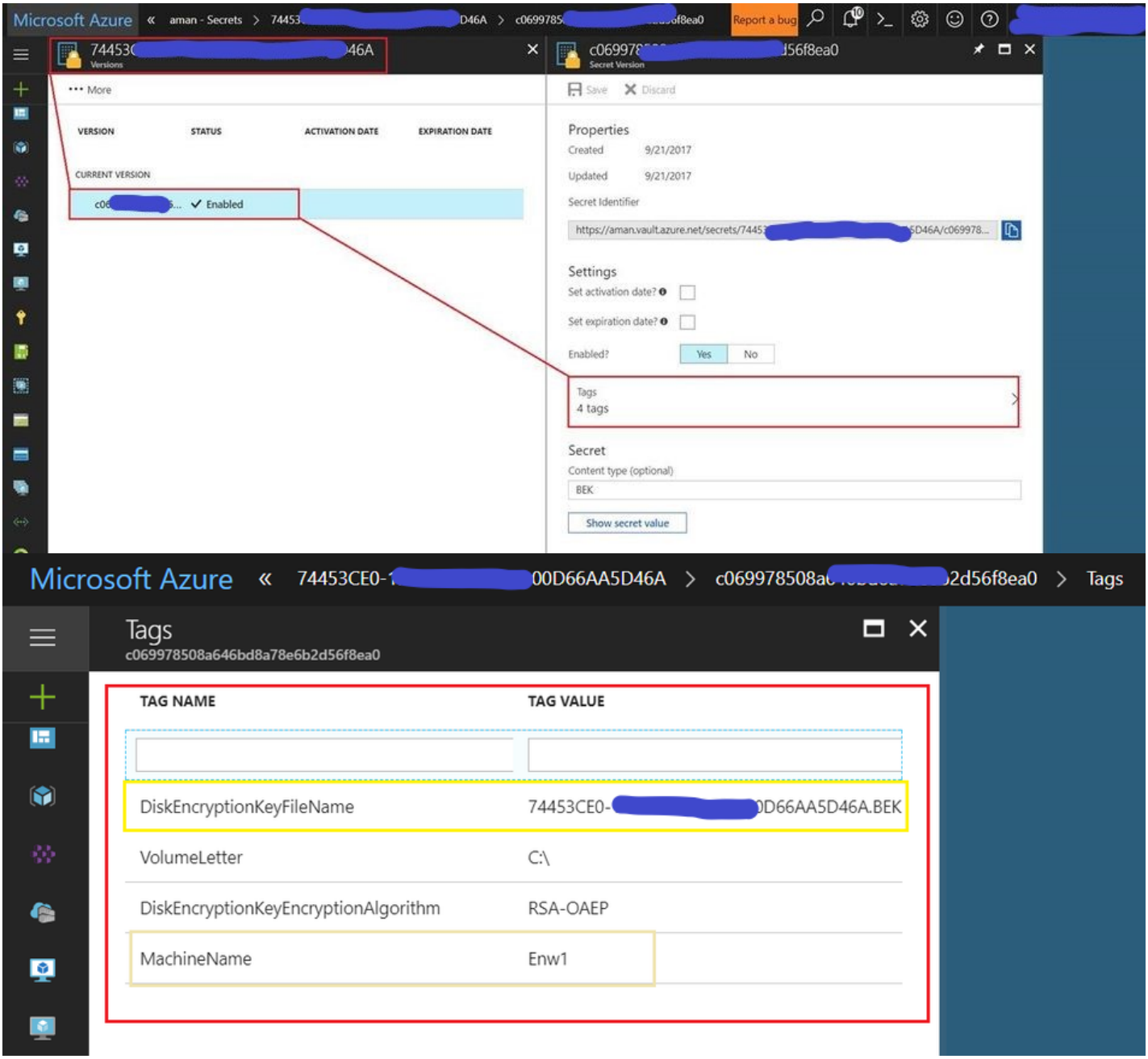
4. The third way to check is by viewing it in the Keyvault from the portal:

5. The extension for Windows VMs creates the following Tags for the Secret which makes it easy for us to identify the Secret used by a particular VM.

   - MachineName
   - VolumeLetter

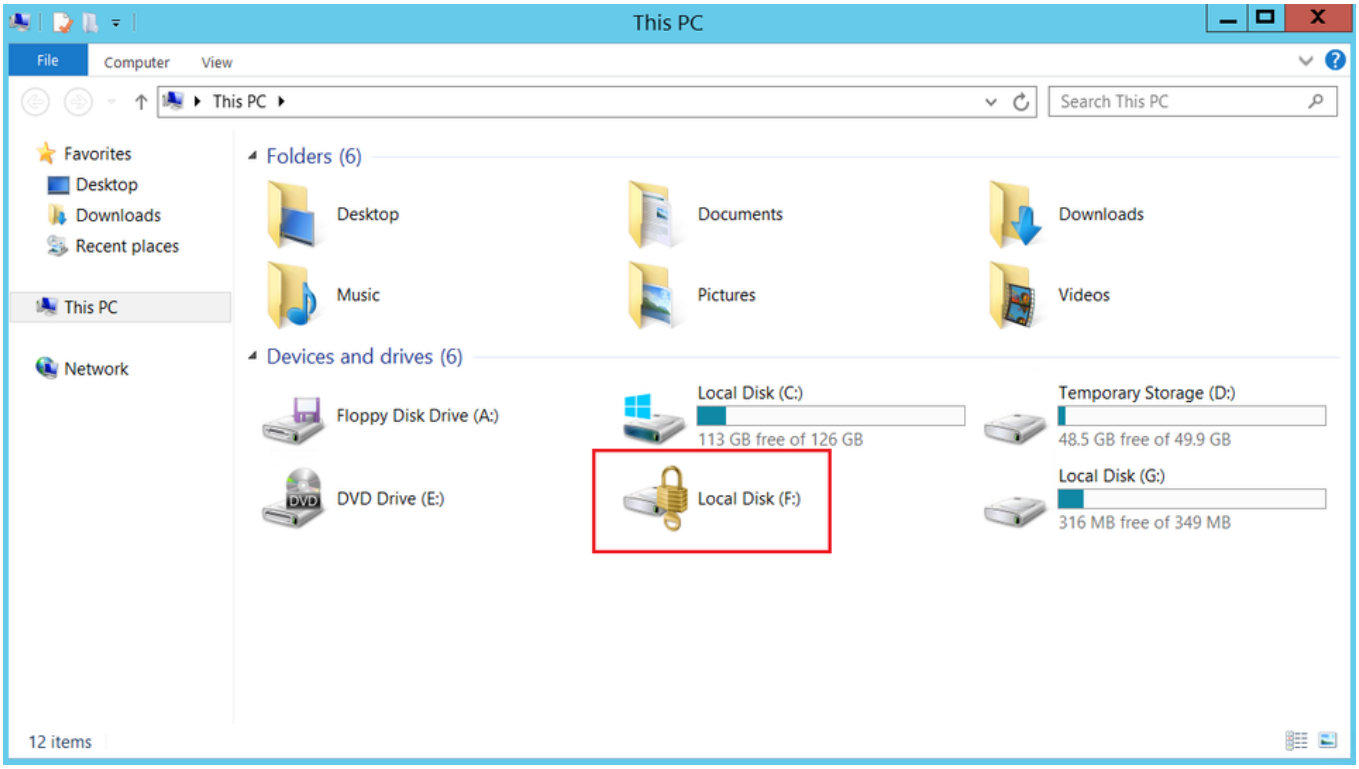
   Note: These tags are only applicable for Windows VM. For Linux VMs, the extension does not create these tags.





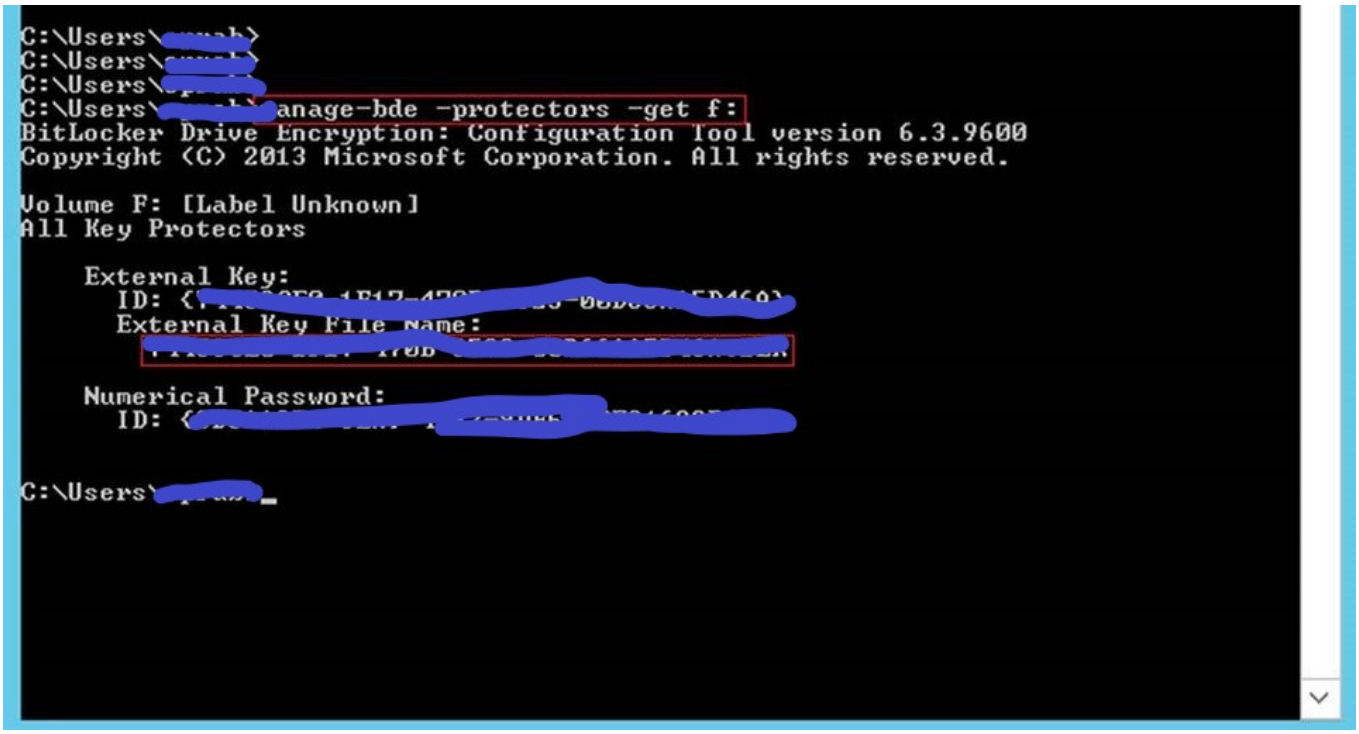
6. From the Guest OS:

    1. Attach the disk as data disk to another VM. Once attached to the VM, the explorer window will look like the one below. The encrypted drive will have a lock icon.

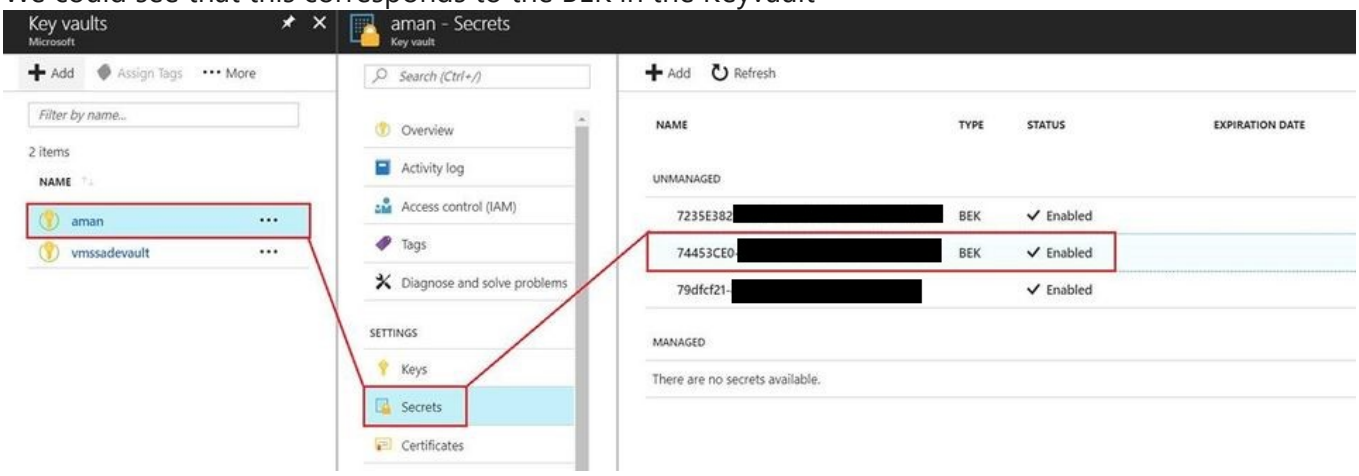


2. Open command prompt with administrator privileges and run the following command:

```
manage-bde -protectors -get <volume letter>
```



3. We could see that this corresponds to the BEK in the Keyvault



4. We can also use the following PowerShell commands to retrieve the secret against the VM name:

```
$rgName = "<RESOURCE GROUP>"
$kvrgName = 'ToTestEncryption'
$vmName = "<VM NAME>"
$KeyVaultName = "<KEY VAULT NAME>"
$keyvaultkeyname = "<KEY NAME>"
$location = "<LOCATION>"

Get-AzKeyVaultSecret -VaultName $keyvaultName | where {($_.Tags.MachineName -eq "$vmName") -and
```

```
PS C:\User Get-AzureKeyVaultSecret -VaultName $keyvaultName | where {($_.Tags.MachineName -eq "$vmName") -and ($_.ContentType -match 'BEK')}

Vault Name   :
Name         : 74453CE0-
Version      :
Id           : https://aman.vault.azure.net:443/secrets/74453CE0-
Enabled      : True
Expires      :
Not Before   :
Created      : 9/21/2017 2:11:10 PM
Updated      : 9/21/2017 2:11:10 PM
Content Type : BEK
Tags         : Name                                Value
               VolumeLetter                        C:\
               MachineName                         Enw1
               DiskEncryptionKeyFileName           74453CE0-1F17-
               DiskEncryptionKeyEncryptionAlgorithm RSA-OAEP
```

Conclusion

This way we can find which SECRET is being used and then proceed to the next steps to recover the BEK file from the keyvault to unlock the VHD.

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!